PUBLIC

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

DOCKET NO. 9357

In the Matter of

LabMD INC.,
a corporation

Respondent.

INITIAL DECISION

D. Michael Chappell
Chief Administrative Law Judge

Date: November 13, 2015

TABLE OF CONTENTS

I. INTRODUCTION 1
A. SUMMARY OF COMPLAINT AND ANSWER 1
1. The Complaint 1
2. Respondent's Answer and Defenses 2
B. PROCEDURAL HISTORY 5
1. Overview 5
2. Procedural Summary 6
C. EVIDENCE 11
D. SUMMARY OF INITIAL DECISION 13

II. FINDINGS OF FACT 15
A. KEY TERMS 15
B. TESTIFYING EXPERTS 15
1. Complaint Counsel's Experts 15
a. Dr. Raquel Hill 15
b. Mr. Rick Kam 16
c. Mr. James Van Dyke 16
d. Dr. Clay Shields 17
2. Respondent's Expert 17
a. Mr. Adam Fisk 17
C. RESPONDENT 18
1. Background Information 18
2. Collection of Personal Information in Connection with Lab Testing 20
3. Insurance Aging Reports 21
4. Collection of Personal Information in Connection with Payments 22
D. THE 1718 FILE INCIDENT 22
1. Peer-to-Peer Networks 22
2. The 1718 File 24
a. Background facts 24
b. LabMD discovery 25
3. Tiversa 26
a. Tiversa's business 26
b. Tiversa's dealings with LabMD 29
c. Tiversa's role as source for FTC investigation 30
d. CX0019 32
4. Credibility Findings Concerning the 1718 File Incident 33
5. Professor Eric Johnson 34
E. THE SACRAMENTO INCIDENT 36
1. Sacramento Police Department's Discovery of LabMD Documents 36
2. Connection between the Sacramento Documents and LabMD's Computer Network 37
3. Follow up to Discovery of the Sacramento Documents 39
4. Lack of Foundation for Admission of CX0451 39
F. IDENTITY THEFT HARM 41

III. ANALYSIS 45
A. BURDEN OF PROOF 45
B. JURISDICTION 46
C. LEGAL FRAMEWORK FOR DETERMINING UNFAIR CONDUCT 47
D. CONSUMER HARM ANALYSIS 49
1. Terminology 49
2. Overview of Arguments on Substantial Consumer Injury 50
3. Actual or Likely Harm 52
4. Complaint Counsel's Proffered Consumer Injury Experts 56
5. The 1718 File Incident 57
a. Summary of facts 57
b. Overview of analysis 59
c. Identity theft harm 60
i. Mr. Rick Kam 60
ii. Mr. James Van Dyke 62
d. Medical identity theft harm 66
e. Reputational and other harms 68
f. Conclusion 69
6. The Sacramento Incident 70
a. Summary of facts 70
b. Summary of arguments 71
c. Connection to LabMD's computer network 72
d. Identity theft harm 75
i. Mr. Rick Kam 75
(a) Opinions 75
(b) Exclusion of CX0451 76
ii. Mr. James Van Dyke 79
e. Conclusion 80
7. Risk of Harm to Consumers whose Personal Information is Maintained on LabMD's Computer Network 80
a. Introduction 80
b. Analysis 82
c. Conclusion 87
E. CONCLUSION 87

IV. SUMMARY OF CONCLUSIONS OF LAW 89

ORDER 92

I. INTRODUCTION

A. SUMMARY OF COMPLAINT AND ANSWER

1. The Complaint

The Administrative Complaint in this case ("Complaint"), issued by the Federal Trade Commission ("FTC" or "Commission") on August 28, 2013, charges that Respondent LabMD, Inc. ("Respondent" or "LabMD"), a clinical testing laboratory, failed to provide "reasonable and appropriate" security for personal information maintained on LabMD's computer networks, and that this conduct "caused or is likely to cause" substantial consumer injury. Therefore, the Complaint alleges, Respondent is liable for "unfair" acts or practices under Section 5(a) of the Federal Trade Commission Act ("FTC Act"). Complaint ¶¶ 10, 17-21, 22-23.

Specifically, the Complaint alleges that "[R]espondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." Complaint ¶ 10. "Among other things," according to the Complaint, Respondent:

(a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information;
(b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks;
(c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
(d) did not adequately train employees to safeguard personal information;
(e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures;
(f) did not maintain and update operating systems of computers and other devices on its networks; and
(g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks.

Complaint ¶ 10(a)-(g).

The Complaint alleges two "security incidents" occasioned by Respondent's alleged unreasonable data security. The first incident, according to the Complaint, occurred in May 2008, when a "third party" informed Respondent that a June 2007 insurance aging report was "available" on a peer-to-peer ("P2P") file-sharing network, through a file-sharing application

called LimeWire. Complaint ¶ 17. The insurance aging report allegedly contained personal information, such as names, dates of birth, Social Security numbers ("SSNs"), current procedural terminology ("CPT") codes, and health insurance company names, addresses, and policy numbers, for approximately 9,300 patients of LabMD's physician clients. Complaint ¶ 19. This insurance aging report, consisting of 1,718 pages, is referred to herein as the "1718 File."

For the second alleged security incident asserted to have been caused by Respondent's alleged failure to protect data on its computer networks, the Complaint alleges that in October 2012, "more than 35 Day Sheets" and "a small number of copied checks" were found in the possession of individuals who subsequently pleaded "no contest" to identity theft charges (the "Sacramento Documents"). Complaint ¶ 21. The Complaint further claims that the Sacramento Documents included personal information such as names and Social Security numbers, and that some of the Social Security numbers have been used by people with different names, which the Complaint alleges indicates use of Social Security numbers by identity thieves. Complaint ¶ 21.

The Complaint concludes that Respondent's alleged failure to employ "reasonable and appropriate" measures to prevent unauthorized access to personal data caused, or is likely to cause, substantial harm to consumers that is not reasonably avoidable by consumers or outweighed by benefits to consumers or competition, and therefore constitutes an unfair practice under Section 5 of the FTC Act. Complaint ¶¶ 22, 23.

2. Respondent's Answer and Defenses

Respondent filed its Answer and Defenses to the Complaint on September 17, 2013. By Order issued July 27, 2015, Respondent was granted leave to add an additional affirmative defense, and Respondent filed its First Amended Answer and Defenses on July 31, 2015 ("Amended Answer"). The Amended Answer denies all material allegations of the Complaint, except as noted below.

Respondent's Amended Answer admits that it is a Georgia corporation, and further states that it is a clinical laboratory that conducts tests on specimen samples and reports the test results to authorized physicians. Amended Answer ¶¶ 1, 3. Respondent further admits that it files insurance claims for the testing charges with health insurers. Amended Answer ¶ 4. In

connection with the foregoing activities, Respondent receives patient names, addresses, dates of birth, gender, telephone numbers, Social Security numbers, lab tests and lab testing codes, and health insurance company names and policy numbers. Amended Answer ¶ 6. Respondent further admits that it uses a computer network in its business to file insurance claims and prepare bills, and that it creates spreadsheets that may include patient information and insurance information. Amended Answer ¶ 9.

With respect to the alleged security incidents set forth in the Complaint, Respondent's Amended Answer states that Tiversa Holding Company ("Tiversa") contacted LabMD in May 2008 claiming to have obtained the 1718 File through LimeWire. Amended Answer ¶ 17. Respondent further states its belief that LimeWire had been downloaded and may have been installed on a computer used by LabMD's billing department manager "no later than" 2006. Amended Answer ¶ 18.

The Amended Answer includes six defenses, including: the Complaint fails to state a valid claim; the Commission lacks subject matter jurisdiction over the claims made in this case; the Commission lacks statutory authority to regulate the acts and practices alleged in the Complaint, making the Commission's actions unlawful; the alleged acts and practices have not caused, and are not likely to cause, substantial injury that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition; the enforcement action against Respondent violates Respondent's due process rights because the Commission has not provided fair notice of the data security standards that the Commission believes Section 5 prohibits or requires; and, the claims alleged in the Complaint are barred by Article II of the United States Constitution because the presiding Administrative Law Judge ("ALJ") is an "inferior officer" that has not been properly appointed by the Commissioners of the FTC, the President, or the Judiciary (the "Appointments Clause" defense). Amended Answer at 5-6.

Respondent presented each of the foregoing defenses, other than the Appointments Clause defense, in a pre-trial Motion to Dismiss filed November 12, 2013. Under the

Commission's Rules of Practice, the Motion was decided by the Commission[1] – the same entity that, when issuing the Complaint, stated it had "reason to believe" that LabMD violated the provisions of the FTC Act. Complaint at 1. The Commission rejected Respondent's defenses, holding that the statutory prohibition against unfair trade practices in Section 5 could be applied to allegedly unreasonable and injurious data security practices, and declined to dismiss the Complaint. *In re LabMD, Inc.*, 2014 FTC LEXIS 2 (Jan. 16, 2014) ("Commission Order on Motion to Dismiss").

In addition, Respondent filed a pre-trial Motion for Summary Decision on April 21, 2014, which, like Respondent's pre-trial Motion to Dismiss, was also decided by the Commission, pursuant to the Commission's 2009 Rule changes. *See* footnote 1. The Commission denied Respondent's Motion for Summary Decision, holding that there were genuine disputes about some of the factual issues raised by LabMD and that LabMD's liability "for engaging in 'unfair acts or practices' in violation of . . . 15 U.S.C. § 45(a) . . . must be resolved based on factual evidence presented at an evidentiary hearing." *In re LabMD, Inc.*, 2014 FTC LEXIS 126, at *1-2 (May 19, 2014).[2]

[1] The Commission amended Rule 3.22 of its Rules of Practice in 2009 to allow "the Commission to decide legal questions and articulate applicable law when the parties raise purely legal issues." Proposed rule amendments; request for public comment, 73 Fed. Reg. 58,832, 58,836 (Oct. 7, 2008). "[C]ommenters (including the [Section of Antitrust Law of the American Bar Association ('Section')], criticized the [Commission's] proposed Rule change as unfairly invading the province of the independent ALJ and compromising the Commission's dual roles as prosecutor and adjudicator." Interim final rules with request for comment, 74 Fed. Reg. 1804, 1809 (Jan. 13, 2009). "For example, the Section argued that the proposed changes . . . could raise concerns about the impartiality and fairness of the Part 3 proceeding by permitting the Commission to adjudicate dispositive issues, including motions to dismiss challenging the facial sufficiency of a complaint, shortly after the Commission has voted out the complaint finding that it has 'reason to believe' there was a law violation, without the benefit of an opinion by an independent ALJ." *Id.* A joint comment from former FTC Chairman Robert Pitofsky and Michael N. Sohn "similarly argued that the proposed rules, including Rule 3.22, would arguably infringe on the fairness of the Part 3 proceeding if the Commission more frequently 'invades what has heretofore been the province of an independent ALJ.'" *Id.* Dismissing these objections, the Commission amended its Rules of Practice to give to itself the authority to decide "[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision[.]" 16 C.F.R. § 3.22(a).

[2] On December 17, 2013, Respondent filed a Motion to Disqualify Commissioner Brill from participating in this administrative proceeding, arguing that, based on her comments in two public speeches, Commissioner Brill had prejudged the facts of this case. Commissioner Brill issued a statement denying that she had prejudged the case, but concluding nevertheless that, to avoid an undue distraction from the issues raised in the Commission's Complaint against LabMD, she would recuse herself from further participation in the matter. *In re LabMD, Inc.*, 2013 FTC LEXIS 138 (Dec. 24, 2013). Respondent also filed two motions seeking to disqualify Commission Chairwoman Ramirez from participating further in this matter. By Orders dated June 15, 2015 and August 14, 2015, the Commission denied those motions. *In re LabMD, Inc.*, 2015 FTC LEXIS 142 (June 15, 2015); *In re LabMD, Inc.*, 2015 FTC LEXIS 185 (Aug. 14, 2015).

Further, concurrent with its Motion to File an Amended Answer to add the Appointments Clause defense, Respondent filed a Motion to Dismiss based on the Appointments Clause defense, the resolution of which the Administrative Law Judge had, on the record, deferred to the Initial Decision. Tr. 1492-1493, 1497-1502. The Commission, exercising its "plenary authority over this adjudication," denied Respondent's Motion to Dismiss based on the Appointments Clause defense, holding "that the Appointments Clause does not apply to the hiring of Commission administrative law judges." However, in order to "put[] to rest any possible claim that this administrative proceeding violates the Appointments Clause," the Commission "ratified Judge Chappell's appointment as a Federal Trade Commission administrative law judge and as the Commission's Chief Administrative Law Judge." *In re LabMD, Inc.*, 2015 FTC LEXIS 215, at *4-6 (Sept. 14, 2015) and Exhibit A thereto (FTC Minute dated September 11, 2015).

B. PROCEDURAL HISTORY

1. Overview

The evidentiary hearing began on May 20, 2014. FTC Complaint Counsel ("Complaint Counsel") rested its case on May 23, 2014. As more fully described below, completion of Respondent's case was delayed by proceedings to obtain prosecutorial immunity for a defense witness, and the case was reconvened on May 5, 2015. After completion of Respondent's witnesses and resolution of certain evidentiary motions,[3] the evidentiary hearing was completed on July 15, 2015. The hearing record was closed by Order dated July 20, 2015.[4]

Rule 3.51(a) of the Commission's Rules of Practice states that "[t]he Administrative Law Judge shall file an initial decision within 70 days after the filing of the last filed initial or reply proposed findings of fact, conclusions of law and order . . . ." 16 C.F.R. § 3.51(a). The parties filed concurrent post-trial briefs and proposed findings of fact on August 10, 2015. The parties filed replies to the other's proposed findings of fact and post-trial briefs on September 4, 2015.

[3] *See In re LabMD, Inc.*, 2015 FTC LEXIS 175 (July 15, 2015); *In re LabMD, Inc.*, 2015 FTC LEXIS 154 (June 22, 2015).

[4] Over 1,080 exhibits were admitted into evidence, 39 witnesses testified, either live or by deposition, and there are 1,504 pages of trial transcript. The parties' proposed findings of fact and conclusions of law, post-trial briefs, replies to proposed findings of fact and conclusions of law, and reply briefs total 2,066 pages.

Pursuant to Commission Rule 3.41(b)(6), closing arguments were held on September 16, 2015. Seventy days from the last filed reply proposed findings and conclusions of law and reply briefs is November 16, 2015.

2. Procedural Summary

Proceedings in this matter have been lengthy, with over 200 entries on the docket, including, among other filings, numerous discovery motions, sanctions motions, and motions to dismiss filed before and after commencement of the evidentiary hearing.[5] A detailed history is available on the FTC's website at https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter, and in the interest of brevity will not be repeated here. Instead, the following procedural summary focuses on certain events in the evolution of the case that have led to the unusual result of Complaint Counsel retreating from its own evidence – evidence upon which it had relied in substantial part to support its claim of consumer injury in this case – as explained below.

By way of background, the FTC commenced its investigation into LabMD's data security practices in 2010, based upon Tiversa's claim that the 1718 File, containing personal information, had been disclosed by means of a peer-to-peer file-sharing network. *See* Fed. Trade Comm'n, "Widespread Data Breaches uncovered by FTC Probe" (Feb. 22, 2010), *at* https://www.ftc.gov/news-events/press-releases/2010/widespread-data-breaches-uncovered-ftc-probe; *see also* Letter from Commissioner Brill Denying Motion to Limit or Quash Civil Investigative Demand, April 20, 2012 at 2, *at* https://www.ftc.gov/sites/ default/files/ documents/petitions-quash/labmd-inc./102-3099-lab-md-letter-ruling-04202012.pdf. Dissenting from the above-cited letter by Commissioner Brill denying Respondent's Motion to Quash or Limit Civil Investigative Demand, then-Commissioner Rosch warned against relying on information provided by Tiversa, stating that "Tiversa is more than an ordinary witness, informant, or 'whistle-blower.' It is a commercial entity that has a financial interest in

[5] At the conclusion of evidence presented by Complaint Counsel, Respondent moved to dismiss the Complaint for failure of Complaint Counsel's evidence to establish a *prima facie* case of unfair trade practices. By Order issued after the close of the record on July 21, 2015, Respondent's motion was denied. *In re LabMD, Inc.*, 2015 FTC LEXIS 182 (July 21, 2015). On April 24, 2015, Respondent filed another motion to dismiss, arguing that Complaint Counsel engaged in "misconduct and indiscretions" in the investigation and prosecution of this case, including with respect to its reliance on evidence provided by Tiversa, a motion which was also denied as premature. *In re LabMD, Inc.*, 2015 FTC LEXIS 122 (May 26, 2015).

intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations." Dissenting Statement of Commissioner J. Thomas Rosch re FTC File No. 1023099 (June 21, 2012) at 1, *at* https://www.ftc.gov/sites/default/files/documents/ petitions-quash/labmd-inc./1023099-labmd-full-commission-review-jtr-dissent.pdf. Former Commissioner Rosch further noted that, according to LabMD, after Tiversa's discovery of the 1718 File on a peer-to-peer network in 2008, Tiversa "repeatedly solicited LabMD, offering investigative and remediation services regarding the breach, long before Commission staff contacted LabMD." *Id.* at 1-2. Former Commissioner Rosch advised that, under these circumstances, the FTC staff should not inquire about the 1718 File, and should not rely on Tiversa for evidence or information, in order to avoid the appearance of impropriety. *Id.*

FTC staff did not heed then-Commissioner Rosch's warning, and also did not follow his advice. Instead, Complaint Counsel chose to further commit to and increase its reliance on Tiversa. During discovery, Complaint Counsel subpoenaed deposition testimony and documents from Tiversa through Tiversa's chief executive officer and deposition designee, Mr. Robert Boback, and then relied on this evidence to claim that the 1718 File, which formed the basis for one of the two "security incidents" alleged in the Complaint, "has been found on a public P2P network as recently as November 2013. It has been downloaded from four different Internet Protocol ('IP') addresses, including IP addresses with 'unrelated sensitive consumer information that could be used to commit identity theft.'"[6] Complaint Counsel's Pre-Trial Brief at 49 (citing CX0703 (Boback Dep.)). Complaint Counsel gave this Tiversa-provided information to its proffered consumer injury expert witness, Mr. Rick Kam, who relied on that information to support his opinion that consumers identified in the 1718 File are at "a significantly higher risk of identity crimes than the general public." CX0742 (Kam Expert Report at 18-19). Complaint Counsel's other proffered consumer injury expert, Mr. James Van Dyke, also relied on Mr.

[6] Although Complaint Counsel marked this statement in its Pre-Trial Brief as subject to *in camera* treatment, the substance of this statement does not meet the Commission's strict standards for *in camera* treatment. The ALJ may disclose *in camera* material to the extent necessary for the proper disposition of the proceeding. 16 C.F.R. § 3.45(a); *In re General Foods Corp.*, 95 F.T.C. 352, 356 n.7, 1980 FTC LEXIS 99, at *11 n.7 (March 10, 1980) (ALJs "retain the power to reassess prior *in camera* rulings at the time of publication of decisions."). In instances where a document or trial testimony had been given *in camera* treatment, but the portion of the material cited to in this Initial Decision does not in fact require *in camera* treatment, such material is disclosed in this public Initial Decision.

Boback's 2013 deposition testimony to support his projections of likely identity theft harm arising from the exposure of the 1718 File. CX0741 (Van Dyke Expert Report at 7-8, 12-14).

The credibility and reliability of evidence provided by Tiversa regarding the "spread" of the 1718 File, including to IP addresses allegedly belonging to identity thieves, began to unravel on May 30, 2014, shortly after Complaint Counsel had rested its case. Complaint Counsel announced in court that it had identified "a discrepancy" and a "misstatement on the record" of Mr. Boback's deposition "on which certain of our experts relied in making [consumer harm] calculations." Tr. 1227, *in camera*. Complaint Counsel requested to redepose Mr. Boback to allow him to revise his prior deposition testimony, and also requested leave to allow Complaint Counsel's consumer injury experts to revise their expert opinions based on Mr. Boback's anticipated revised testimony. These requests, made in the middle of trial, long after discovery had closed, and, indeed, after Complaint Counsel had rested its case, were denied. Tr. 1227-1229, *in camera*.[7]

Also on May 30, 2014, counsel for Respondent reported that the House Committee on Oversight and Government Reform ("OGR") had begun an investigation of Tiversa in conjunction with Tiversa's work with federal government agencies, and that Respondent's proposed witness for May 30, 2014, Tiversa's former employee, Mr. Richard Wallace, had just been informed by OGR that OGR was seeking to interview Mr. Wallace. Tr. 1225, *in camera*; *see* JX0003. It was further disclosed that, if called to testify in the administrative proceedings, Mr. Wallace would invoke his constitutional privilege against self-incrimination, pending his

[7] Complaint Counsel further explained in court: "it is also the representation of Mr. Boback's counsel that he has looked for the [1718 F]ile more recently and found it more recently, and on that basis we would seek to take a second deposition of Mr. Boback." Tr. 1227-1228, *in camera*. Complaint Counsel's explanation in court clearly indicated that Mr. Boback's "misstatement" was in regard to *when* Tiversa allegedly searched peer-to-peer networks and found the 1718 File in "multiple locations" and not *whether* Tiversa had in fact located the file in "multiple locations." Moreover, notwithstanding the denial of Complaint Counsel's request to redepose Mr. Boback, Complaint Counsel, over Respondent's objection, elicited testimony from Mr. Boback at Respondent's June 7, 2014 trial deposition of Mr. Boback (a deposition which was allowed due to Mr. Boback's alleged unavailability to appear at trial (Tr. 1251-1252)), that Tiversa ran a search for the 1718 File on June 3 or 4, 2014, and identified three IP addresses from which the 1718 File had been downloaded, in addition to the four IP addresses on CX0019 (discussed *infra* II.D.3.). RX0541 (Boback Trial Dep.) at 78. Because, as shown *infra*, Mr. Boback's testimony in this case is not credible, and evidence produced by Tiversa is not reliable as to the "spread" of the 1718 File, ultimately such "clarifying" testimony or evidence from Mr. Boback on this issue would not have been entitled to, or given, any weight.

effort to obtain a grant of prosecutorial immunity. Tr. 1225, 1231-1232, 1241-1242, *in camera*; *see* 16 C.F.R. § 3.39.

On June 12, 2014, counsel for Respondent stated on the record that Mr. Wallace was expected to testify in this case that the Tiversa-provided evidence that the 1718 File had been found at four IP addresses other than LabMD's, including IP addresses of identity thieves, had been manufactured, and that, in fact, the 1718 File had not been found at any IP address other than LabMD's. Tr. 1293. Also on June 12, 2014, Mr. Wallace took the stand and invoked his privilege against self-incrimination in response to Respondent's questioning. Tr. 1301-1302.

Proceedings were recessed to allow Mr. Wallace to seek prosecutorial immunity for the OGR testimony and for testimony in these administrative proceedings. *In re LabMD, Inc.*, 2014 FTC LEXIS 246 (Oct. 9, 2014). On December 29, 2014, on Respondent's motion, and pursuant to authority granted by the Attorney General of the United States on November 14, 2014, an Order was issued granting Mr. Wallace immunity pursuant to Commission Rule 3.39 and directing Mr. Wallace to testify in these proceedings. *See In re LabMD, Inc.*, 2014 FTC LEXIS 314 (Dec. 29, 2014). Proceedings reconvened for Mr. Wallace's testimony on May 5, 2015.[8]

On May 5, 2015, Mr. Wallace appeared and testified. As detailed in Section II.D.3., *infra*, Mr. Wallace testified that Tiversa's business model was to "monetize" documents that it downloaded from peer-to-peer networks, by using those documents to sell data security remediation services to the affected business, including by representing to the affected business that the business' information had "spread" across the Internet via peer-to-peer sharing networks, when such was not necessarily the case, and by manipulating Tiversa's internal database of peer-to-peer network downloads (the "Data Store") to make it appear that a business' information had been found at IP addresses belonging to known identity thieves. Mr. Wallace further testified that these practices were followed with regard to Tiversa's discovery of LabMD's 1718 File. In order to retaliate against LabMD for refusing to purchase Tiversa's services, Mr. Wallace

[8] Although proceedings were to reconvene on March 3, 2015, Mr. Wallace was granted two continuances. *See* Orders of February 24, 2015 and March 4, 2015. On March 12, 2015, the Administrative Law Judge ordered a further continuance *sua sponte* until May 5, 2015.

testified, Tiversa reported its discovery of the 1718 File to the FTC; and Mr. Wallace, at the direction of Mr. Boback, manipulated Tiversa's Data Store to make it appear that the 1718 File had been found at four IP addresses, including IP addresses of known identity thieves, and fabricated a list of those IP addresses, which Complaint Counsel introduced into evidence as CX0019.

Complaint Counsel opted not to take Mr. Wallace's deposition after his direct testimony. Tr. 1459. That deposition had been allowed by Order issued December 8, 2014. *In re LabMD, Inc.*, 2014 FTC LEXIS 307 (Dec. 8, 2014). Complaint Counsel also chose not to cross-examine Mr. Wallace. Tr. 1459. Complaint Counsel further decided not to offer any rebuttal to Mr. Wallace's testimony. Tr. 1459. *See* Complaint Counsel's Notice Regarding Rebuttal, May 12, 2015.[9]

Meanwhile, the OGR's investigation of Tiversa continued, including with respect to Tiversa's dealings with the FTC in this case. *See* RX0542; RX0543. An OGR staff report, dated January 2, 2015, but not released until after the completion of Mr. Wallace's testimony in this matter, concluded, *inter alia*, that Tiversa and Mr. Boback provided incomplete, inconsistent, and/or conflicting information to the FTC for this case. *See* RX0644; *see also In re LabMD, Inc.*, 2015 FTC LEXIS 175 (July 15, 2015).

On June 24, 2015, Complaint Counsel announced for the first time that it "does not intend to cite to Mr. Boback's testimony or CX0019 in its proposed findings of fact. Nor does Complaint Counsel intend to cite to expert conclusions predicated on Mr. Boback's testimony or CX0019." Complaint Counsel's Opposition to Respondent's Motion to Admit Exhibits at 10-11 n.11. *See also* Complaint Counsel's Response to Respondent's Motion to Refer Tiversa and Boback for Criminal Investigation at 2 n.1 (July 1, 2015).[10] Complaint Counsel further explained its retreat from Tiversa-provided evidence in its Post-Trial Brief, stating: "The

[9] Complaint Counsel's Motion to Issue Subpoenas to Tiversa to develop rebuttal evidence, filed July 8, 2014, before Mr. Wallace's testimony and while Mr. Wallace's request for immunity was still pending with the Attorney General, had been denied as premature. *In re LabMD, Inc.*, 2014 FTC LEXIS 194 (July 23, 2014).

[10] Complaint Counsel did not oppose a criminal referral of Tiversa and Mr. Boback; however, Respondent's motion for such referral was denied for failure to provide sufficient legal authority. *In re LabMD, Inc.*, 2015 FTC LEXIS 177 (July 15, 2015).

assertions made on page 49 of Complaint Counsel's pre-trial brief are not repeated here. Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony." Complaint Counsel's Post-Trial Brief at 61 n.3.[11] However, as shown *infra*, Complaint Counsel does rely on expert opinions that were predicated on Mr. Boback's testimony. In addition, Complaint Counsel relies on Mr. Boback's deposition testimony to counter Respondent's Proposed Findings of Fact. *See, e.g.*, CCRRFF 72b, 73b, 74b.

C. EVIDENCE

This Initial Decision is based on a consideration of the whole record relevant to the issues, including the exhibits properly admitted into evidence, deposition transcripts, and the transcripts of testimony at trial, and addresses the material issues of fact and law. The briefs and proposed findings of fact and conclusions of law, and the replies thereto, submitted by the parties, and all contentions and arguments therein were thoroughly reviewed and considered.

Proposed findings of fact submitted by the parties but not accepted in this Initial Decision were rejected, either because they were not supported by the evidence or because they were not dispositive or material to the determination of the merits of the case. Similarly, legal contentions and arguments of the parties that are not addressed in this Initial Decision were rejected, because they lacked support in fact or law, were not material, or were otherwise lacking in merit.[12]

[11] The parties filed corrected versions of some of their post-trial filings, as indicated in footnote 13. Citations in this Initial Decision to those filings are to the corrected version of the filing.

[12] Ruling upon a decision of the Interstate Commerce Commission, and interpreting language in the Administrative Procedure Act that is almost identical to language in FTC Rule 3.51(c)(1), the United States Supreme Court held that "[b]y the express terms of [that Act], the Commission is not required to make subordinate findings on every collateral contention advanced, but only upon those issues of fact, law, or discretion which are 'material.'" *Minneapolis & St. Louis Ry. Co. v. United States*, 361 U.S. 173, 193-94 (1959). *Accord Stauffer Labs., Inc. v. FTC*, 343 F.2d 75, 82 (9th Cir. 1965). *See also Borek Motor Sales, Inc. v. NLRB*, 425 F.2d 677, 681 (7th Cir. 1970) (holding that it is adequate for the Board to indicate that it had considered each of the company's exceptions, even if only some of the exceptions were discussed, and stating that "[m]ore than that is not demanded by the [APA] and would place a severe burden upon the agency"). Furthermore, the Commission has held that Administrative Law Judges are not required to discuss the testimony of each witness or all exhibits that are presented during the administrative adjudication. *In re Amrep Corp.*, 102 F.T.C. 1362, 1670, 1983 FTC LEXIS 17, at *566-67 (Nov. 2, 1983).

Under Commission Rule 3.51(c)(1), "[a]n initial decision shall be based on a consideration of the whole record relevant to the issues decided, and shall be supported by reliable and probative evidence." 16 C.F.R. § 3.51(c)(1); *see In re Chicago Bridge & Iron Co.*, 138 F.T.C. 1024, 1027 n.4, 2005 FTC LEXIS 215, at *3 n.4 (Jan. 6, 2005). Under the Administrative Procedure Act ("APA"), an Administrative Law Judge may not issue an order "except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the reliable, probative, and substantial evidence." 5 U.S.C. § 556(d). All findings of fact in this Initial Decision are supported by reliable, probative, and substantial evidence. Citations to specific numbered findings of fact in this Initial Decision are designated by "F."[13]

Pursuant to Commission Rule 3.45(b), several orders were issued in this case granting *in camera* treatment to material, after finding, in accordance with the Rule, that its public disclosure would likely result in a clearly defined, serious injury to the entity requesting *in camera* treatment or that the material constituted "sensitive personal information," as that term is defined in Commission Rule 3.45(b). This Initial Decision does not disclose any *in camera* information and there is only a public version of the Initial Decision.

[13] References to the record are abbreviated as follows:

CCX – Complaint Counsel's Exhibit
RX – Respondent's Exhibit
JX – Joint Exhibit
Tr. – Transcript of testimony before the Administrative Law Judge
Dep. – Transcript of Deposition
CCB – Complaint Counsel's Corrected Post-Trial Brief
CCRB – Complaint Counsel's Post-Trial Reply Brief
CCFF – Complaint Counsel's Proposed Findings of Fact
CCRRFF – Complaint Counsel's Reply to Respondent's Proposed Findings of Fact
CCCL – Complaint Counsel's Conclusions of Law
RB – Respondent's Corrected Post-Trial Brief
RRB – Respondent's Post-Trial Reply Brief
RFF – Respondent's Proposed Findings of Fact
RRCCFF – Respondent's Reply to Complaint Counsel's Proposed Findings of Fact
RCL – Respondent's Corrected Conclusions of Law

D. SUMMARY OF INITIAL DECISION

Section 5(n) of the FTC Act states that "[t]he Commission shall have no authority to declare unlawful an act or practice on the grounds that such act or practice is unfair unless [1] the act or practice causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Complaint Counsel has failed to carry its burden of proving its theory that Respondent's alleged failure to employ reasonable data security constitutes an unfair trade practice because Complaint Counsel has failed to prove the first prong of the three-part test – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.

First, with respect to the 1718 File, the evidence fails to prove that the limited exposure of the 1718 File has resulted, or is likely to result, in any identity theft-related harm, as argued by Complaint Counsel. Moreover, the evidence fails to prove Complaint Counsel's contention that embarrassment or similar emotional harm is likely to be suffered from the exposure of the 1718 File alone. Even if there were proof of such harm, this would constitute only subjective or emotional harm that, under the facts of this case, where there is no proof of other tangible injury, is not a "substantial injury" within the meaning of Section 5(n).

Second, with respect to the exposure of certain LabMD "day sheets" and check copies, Complaint Counsel has failed to prove that the exposure of these documents is causally connected to any failure of Respondent to reasonably protect data maintained on its computer network, as alleged in the Complaint, because the evidence fails to show that these documents were maintained on, or taken from, Respondent's computer network. In addition, Complaint Counsel has failed to prove that this exposure has caused, or is likely to cause, any consumer harm.

Third, Complaint Counsel's argument that identity theft-related harm is likely for all consumers whose personal information is maintained on LabMD's computer networks, even if their information has been not exposed in a data breach, on the theory that LabMD's computer networks are "at risk" of a future data breach, is rejected. In summary, the evidence fails to

assess the degree of the alleged risk, or otherwise demonstrate the probability that a data breach will occur. To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical "risk" of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of "likely" substantial consumer injury.

At best, Complaint Counsel has proven the "possibility" of harm, but not any "probability" or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case. Accordingly, the Complaint is DISMISSED. Because Complaint Counsel has failed to prove its case on the merits, it is not necessary to address Respondent's affirmative defenses set forth in the Amended Answer.

II. FINDINGS OF FACT

A. KEY TERMS

1. **1718 File**: The LabMD Insurance Aging report, containing 1,718 pages, with the filename "insuranceaging_6.05.071.pdf" that is identified as the "P2P [peer-to-peer] insurance aging file" in Paragraphs 17, 18, 19, and 21 of the Complaint, a copy of which is designated as CX0697 (*in camera*), and a redacted copy of which is designated at RX0072. (Joint Stipulations of Fact, JX0001-A at 1).

2. **Consumer**: A natural person. The patients of LabMD's physician clients are consumers, as that term is used in Section 5(n) of the Federal Trade Commission Act, 15 U.S.C. § 45(n). (Joint Stipulations of Fact, JX0001-A at 1, 2).

3. **Personal Information ("PI")**: Individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number ("SSN"); (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. (Joint Stipulations of Fact, JX0001-A at 1-2).

B. TESTIFYING EXPERTS

1. Complaint Counsel's Experts

a. Dr. Raquel Hill

4. Dr. Raquel Hill is a tenured professor of computer science at Indiana University with over 25 years of experience in computing, with expertise in computer security, data privacy, and networking systems. (CX0740 (Hill Expert Report ¶ 1)).

5. Dr. Hill has a Ph.D. in computer science from Harvard University. She has designed and taught classes in information and systems security. (CX0740 (Hill Expert Report ¶¶ 8, 9)).

6. Dr. Hill was asked to assess whether LabMD provided reasonable security for Personal Information within its computer network, and whether any alleged security failures could have been corrected using readily available security measures. Specifically, Dr. Hill was asked to analyze the record evidence relating to the allegations in paragraphs 10 and 11 of the Complaint. (CX0740 (Hill Expert Report ¶¶ 2, 45)).

7. Dr. Hill's conclusions in this case are limited to the time period from January 2005 through July 2010 (the "Relevant Time Period"). Dr. Hill found insufficiently "diverse types of information available" after the Relevant Time Period to offer any opinions after the Relevant Time Period, and did not offer any opinions on the reasonableness of LabMD's security practices after July 2010. (CX0740 (Hill Expert Report ¶¶ 4, 48); Hill, Tr. 84-85, 203).

8. Dr. Hill was asked to evaluate and opine on the expert report of Respondent's expert, Mr. Adam Fisk (F. 20). Specifically, Dr. Hill was asked to opine on Mr. Fisk's rebuttal to Dr. Hill's expert report and Mr. Fisk's opinions regarding LabMD's network security practices. (CX0737 (Hill Rebuttal Expert Report) ¶ 2).

b. Mr. Rick Kam

9. Mr. Rick Kam is a Certified Information Privacy Professional. He is president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. (CX0742 (Kam Expert Report at 3)).

10. Mr. Kam leads and participates in cross-industry data privacy groups, 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. Mr. Kam's expertise includes "identifying and remediating the consequences of identity theft and medical identity theft" and "helping organizations develop policies and solutions" to safeguard sensitive personal information. (CX0742 (Kam Expert Report at 3-5, 25, 29-33)).

11. Mr. Kam was asked to "assess the risk of injury to consumers caused by the unauthorized disclosure of [consumers'] sensitive personal information." (CX0742 (Kam Expert Report at 5)).

c. Mr. James Van Dyke

12. Mr. James Van Dyke is the founder and president of Javelin Strategy & Research ("Javelin"), which performs independent research on customer-related security, fraud, payments, and electronic financial services. Mr. Van Dyke has extensive experience in conducting surveys. He leads the publication of an annual, nationally representative victim study of identity crimes in the United States. (Van Dyke, Tr. 574-576, 580-581; CX0741 (Van Dyke Expert Report at 1)).

13. Mr. Van Dyke makes presentations on secure personal financial management, identity fraud, and payments and security to groups including the U.S. House of Representatives, Federal Reserve Bank gatherings, and the RSA Security Conference. (CX0741 (Van Dyke Expert Report at 1)).

14. Mr. Van Dyke's expertise includes consumer behavior, security technologies, personal financial services and payments, how sensitive information is used, and identity theft. (CX0741 (Van Dyke Expert Report at 1-2)).

15. Mr. Van Dyke was asked to "assess the risk of injury to consumers whose personally identifiable information (PII)[14] has been disclosed by [LabMD] without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure." (CX0741 (Van Dyke Expert Report at 2)).

d. Dr. Clay Shields

16. Dr. Clay Shields is a tenured professor in the computer science department of Georgetown University, with expertise in networking and network protocols, computer security, digital forensics, and responding to network and computer system events. (CX0738 (Shields Rebuttal Expert Report ¶ 1)).

17. Dr. Shields has over 20 years of computer science experience, including in digital forensics research and developing and analyzing network protocols. (CX0738 (Shields Rebuttal Expert Report ¶ 5)).

18. Dr. Shields' research includes work on systems for providing anonymity to users through peer-to-peer technology. He was involved in a collaborative effort that resulted in a modified Gnutella client that is widely used by law enforcement.[15] (CX0738 (Shields Rebuttal Expert Report ¶¶ 7, 9)).

19. Dr. Shields was asked to review the expert report of Respondent's expert, Mr. Adam Fisk (F. 20), and provide opinions about Mr. Fisk's conclusions concerning the LimeWire peer-to-peer file-sharing program[16] and the alleged disclosure of the 1718 File. (CX0738 (Shields Rebuttal Expert Report ¶ 2)).

2. Respondent's Expert

a. Mr. Adam Fisk

20. Mr. Adam Fisk is the president and chief executive officer of the Brave New Software Project, Inc., the creators of Lantern, a peer-to-peer tool for bypassing government censors in countries such as Iran and China that censor citizens' access to the Internet. Mr. Fisk is the former lead engineer at LimeWire LLC, the creators of the LimeWire file-

[14] Personally Identifiable Information ("PII") is a subset of the data in Personal Information (F.3) and includes a person's name, address, date of birth, Social Security number, credit card and banking information, and drivers' license number. (CX0742 (Kam Expert Report at 10)).

[15] Peer-to-peer technology and the Gnutella client are discussed *infra* II.D.1.

[16] The LimeWire peer-to-peer file-sharing program is discussed *infra* II.D.1.

sharing application, and has extensive experience in peer-to-peer software, computer networking, and data security, including 13 years of professional experience building peer-to-peer applications, with a focus on computer networking and security. (RX0533 (Fisk Expert Report at 3-4)).

21. Mr. Fisk was asked to provide an opinion as to whether LabMD provided adequate security to secure Protected Health Information[17] contained within its computer network from January 2005 through July 2010 (the "Relevant Time Period" assessed by Dr. Hill). Mr. Fisk also provided his review of LimeWire functionality, an analysis of LabMD's network, an analysis of the 1718 File on the LabMD network, and a rebuttal to the expert report of Dr. Hill. (RX0533 (Fisk Expert Report at 3-4)).

22. Mr. Fisk based his opinions of the facts of this case on his extensive experience and documents provided to him by Respondent. (RX0533 (Fisk Expert Report at 3-4, 37)).

23. In forming his opinions, Mr. Fisk considered an analysis of the equipment LabMD had in place, including whether or not LabMD had firewalls in place, an analysis of the depositions describing the network and the practices in place at the company, and an analysis of a report conducted for LabMD by an outside contractor that looked at any vulnerabilities on LabMD's network. (Fisk, Tr. 1158-1159).

C. RESPONDENT

1. Background Information

24. LabMD is a privately held Georgia corporation, incorporated in 1996 by Mr. Michael J. Daugherty. (Daugherty, Tr. 939; CX0766 at 2).

25. Mr. Daugherty is the sole owner of LabMD and is its president and chief executive officer. (Daugherty, Tr. 936; CX0709 (Daugherty, Dep. at 12)).

26. From at least 2001 through approximately December 2013 or January 2014, LabMD was in the business of conducting clinical laboratory tests on urological specimen samples from patients and reporting test results to physician customers. (Answer ¶ 3; CX0766 at 3; CX0291; Daugherty, Tr. 952).

27. During the period LabMD was operational (F. 26, 39), LabMD operated as a small, medical services company providing uro-pathology cancer detection services to urologists who wanted their patients' tissue samples analyzed by pathologists who specialized in prostate cancer or bladder cancer. (Daugherty, Tr. 941-943, 952).

[17] Protected Health Information, as defined in 45 C.F.R. § 160.103, is a subset of the data in Personal Information. (Joint Stipulations of Fact, JX0001-A at 1, 2).

28. During the period LabMD was operational (F. 26, 39), LabMD tested samples from patients in multiple states, including Alabama, Mississippi, Florida, Georgia, Missouri, Louisiana, and Arizona. (Answer ¶ 5; CX0766 at 3).

29. The patients whose samples LabMD tested and from whom LabMD collected payments were located throughout the United States. (CX0766 at 3; CX0088, *in camera* (LabMD Copied Checks); CX0726 (Maxey, SUN Designee, Dep. at 17); CX0718 (Hudson, Dep. at 15-17); CX0722 (Knox, Dep. at 19); CX0706 (Brown, Dep. at 16-18); CX0715-A (Gilbreth, Dep. at 50-51); CX0713-A (Gardner, Dep. at 25-26)).

30. The acts and practices of Respondent alleged in the Complaint were in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44. (Joint Stipulations of Fact, JX0001-A at 1).

31. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately $35-40 million. (Daugherty, Tr. 1059; CX0709 (Daugherty, Dep. at 127-128)).

32. LabMD's peak annual revenue was approximately $10 million. (CX0709 (Daugherty, Dep. at 128)).

33. From 2005 through 2012, LabMD's approximate blended profit margin was 25%. (Daugherty, Tr. 1058-1059).

34. In 2013, LabMD's revenue was approximately $2 million. (CX0709 (Daugherty, Dep. at 128)).

35. LabMD's principal place of business from April 2009 through approximately January 2014 was 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339. (Answer ¶ 1; CX0766 at 2).

36. In January 2014, LabMD began winding down its operations. At that time, LabMD stopped accepting specimen samples and conducting tests. (CX0765 at 6; CX0710-A (Daugherty, LabMD Designee, Dep. at 195); CX0725-A (Martin, Dep. at 25)).

37. LabMD notified its physician clients by letter dated January 6, 2014, that it would not be accepting new specimens after January 11, 2014, and that all test results would be provided in the following week. LabMD further told its physician clients that LabMD would be closed for telephone calls and internet access after January 15, 2014, and that for the remainder of 2014, requests for past results or to obtain specimens for second opinions, could be made by facsimile. In addition, the January 6, 2014 letter stated, "billing operations" would continue through 2014. (CX0291; Daugherty, Tr. 1031).

38. After January 2014, in order to obtain an historical result report, as referred to in F. 37, the physician client had to send a facsimile requesting the results and LabMD would then fax the report back to the physician client. (CX0725-A (Martin, Dep. at 20)).

39. As of the start of the evidentiary hearing, May 2014, LabMD's operations were limited to preserving tissue samples for LabMD's physician clients, so the physicians could send out slides for second opinions, and to providing test results to physicians if they did not have them. (Daugherty, Tr. 1031; CX0291).

40. LabMD has continued to possess its computer equipment; its "Lytec" server (on which LabMD's electronic billing records are stored); and the laboratory information system (on which LabMD's electronic medical records are stored). Both of these servers can be turned on. (CX0709 (Daugherty, Dep. at 22-23); CX0766 at 2-3). *See also* CX0725-A (Martin, Dep. at 11-12); CX0705-A (Bradley, Dep. at 20)).

41. As of May 2014, LabMD continues to exist as a corporation, with Mr. Daugherty as it sole employee. (Daugherty, Tr. 1031; CX0291).

2. Collection of Personal Information in Connection with Lab Testing

42. In connection with performing tests, LabMD has collected and continues to maintain Personal Information for over 750,000 consumers. (Joint Stipulations of Fact, JX0001-A at 3; CX0765 at 10-11; CX0766 at 5; CX0710-A (Daugherty, LabMD Designee, Dep. at 193-194); CX0709 (Daugherty, Dep. at 21-23)).

43. In connection with performing tests for its physician clients, LabMD's Information Technology ("IT") staff set up data transfer of patients' Personal Information from LabMD's physician clients' databases to LabMD. (CX0718 (Hudson, Dep. at 36-39)).

44. The Personal Information that physicians transferred to LabMD included names, addresses, dates of birth, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and services, and other information. (CX0717 (Howard, Dep. at 34-35, 38); CX0718 (Hudson, Dep. at 59-60, 62); CX0726 (Maxey, SUN Designee, Dep. at 41-42); CX0728 (Randolph, Dep. at 48, 50-51)).

45. Patient Personal Information typically was transmitted to LabMD using a secure file transfer protocol, through which information flowed from the doctors' offices to a LabMD server on its network. (CX0711 (Dooley Dep. at 131-132); CX0730 (Simmons, Dep. at 61, 128); CX0717 (Howard, Dep. at 34-37, 54); CX0724 (Maire, Dep. at 41-43); CX0725-A (Martin, Dep. at 56-60)).

46. Once consumers' Personal Information was loaded in LabMD's laboratory application, LabSoft, staff at the physician clients' practice could order tests for the patients through LabSoft using LabMD's online portal by searching for the patient's name, selecting the correct patient from a list of patients in that practice, and entering the current procedural terminology ("CPT") code for the testing ordered. (CX0718 (Hudson, Dep. at 24-25); CX0709 (Daugherty, Dep. at 86-87); CX0725-A (Martin, Dep. at 56-57)).

47. A doctor's office employee could search by name, date of birth, or Social Security number to find a patient's record to order a test. (CX0726 (Maxey, SUN Designee, Dep. at 40, 47-48)).

48. When a doctor's office made a request for a test, a report and labels for the specimen would be printed at the doctor's office. The patient's specimen and the report were then sent to LabMD via Federal Express. (CX0725-A (Martin, Dep. at 56-57)).

49. Once a LabMD pathologist read a specimen and had a test result, the result was entered into a database. (CX0711 (Dooley Dep. at 132-133); CX0717 (Howard, Dep. at 49-50)).

50. The results from the tests LabMD performed could be accessed by LabMD's physician clients through a web portal using a user ID and password through LabMD-provided computers or the doctors' offices own computers. (CX0726 (Maxey, SUN Designee, Dep. at 29-31, 48-49); CX0728 (Randolph, Dep. at 21-22, 57-58); CX0704-A (Boyle, Dep. at 16, 22-23); CX0722 (Knox, Dep. at 76-78); CX0717 (Howard, Dep. at 59-60); Daugherty, Tr. 977).

51. In some instances, LabMD supplied computer equipment to doctors' offices, including computers, monitors, bar coder machines, and printers. (CX0730 (Simmons, Dep. at 61-62); CX0726 (Maxey, SUN Designee, Dep. at 23-24, 21, 27-28); CX0728 (Randolph, Dep. at 27-31, 42); CX0717 (Howard, Dep. at 59); CX0709 (Daugherty, Dep. at 83)).

3. Insurance Aging Reports

52. Insurance aging reports are spreadsheets of insurance claims and payments, which may include consumers' names, dates of birth, and Social Security numbers; the CPT codes for the laboratory tests conducted; and health insurance company names, addresses, and policy numbers. (Answer ¶ 9(a); CX0706 (Brown, Dep. at 54)).

53. Insurance aging reports were generated by LabMD's billing department to show accounts receivable that had not been paid and so that billing staff could attempt to collect payments on outstanding claims from patients' insurance companies. (CX0706 (Brown, Dep. at 20); CX0714-A ([Former LabMD Employee],[18] Dep. at 48-49)).

54. Insurance aging reports were based on a report from LabMD's Lytec billing system that displayed past-due payments from insurance companies. (CX0706 (Brown, Dep. at 23-24); CX0714-A ([Former LabMD Employee], Dep. at 52)).

55. Insurance aging reports were saved to the billing manager's workstation. (Daugherty, Tr. 982).

[18] By Order dated May 6, 2014, and for the reasons stated therein, *in camera* treatment was granted to the name of one particular former LabMD employee in the billing department. Disclosure of this employee's name is not necessary for the proper disposition of the proceeding and therefore it is replaced with the designation "[the Former LabMD Employee]" in this Initial Decision.

56. [The Former LabMD Employee] (*see* footnote 18) received hard copies of insurance aging reports from LabMD's billing manager every month. Based on the information in the report, the employee would contact the insurance company, obtain the status of the denied claim, and attempt to find ways for the insurance company to pay the claim. (CX0714-A ([Former LabMD Employee], Dep. at 49-50)).

4. Collection of Personal Information in Connection with Payments

57. Insured patients could pay the part of LabMD's charges not covered by insurance, and uninsured patients could be responsible for the full amount of the charges. (Answer ¶ 4).

58. Consumers could pay LabMD's charges with credit cards, debit cards, or personal checks. (CX0766 at 6; CX0706 (Brown, Dep. at 39-40); CX0765 at 8).

59. When consumers paid LabMD by credit card, the billing department ran the credit card number and posted the payment in LabMD's system. (CX0716 (Harris, Dep. at 20-21)).

60. When consumers paid LabMD by check or money order and LabMD received that payment by mail, it was LabMD's practice for LabMD staff to make a photocopy of the check or money order. LabMD did not scan checks or money orders in the 2005 to 2010 time period. (CX0716 (Harris, Dep. at 23-24, 27); CX0706 (Brown, Dep. at 28-29); CX0715-A (Gilbreth, Dep. at 50-51)).

61. When consumers paid LabMD by check or money order, the photocopy (F. 60) would be given to the billing department. The billing department would post the payment and retain the photocopy of the check. Original checks were kept for six months, and then were shredded. (CX0713-A (Gardner, Dep. at 26-27)).

62. Personal checks contain a consumer's account number, bank routing number, signature, and often an address and phone number. (*E.g.*, CX0088, *in camera* (LabMD Copied Checks)).

D. THE 1718 FILE INCIDENT

1. Peer-to-Peer Networks

63. Peer-to-peer file-sharing applications enable one computer user to make a request to search for all files that have been made available for sharing by another (or "host") computer that is also using the file-sharing application. (Hill, Tr. 119-120; Shields, Tr. 826; CX0738 (Shields Rebuttal Expert Report ¶¶ 15, 18)).

64. Peer-to-peer networks are often used to share music, videos, pictures, and other materials. (CX0738 (Shields Rebuttal Expert Report ¶ 14); Answer ¶ 13; CX0740 (Hill Expert Report ¶ 42); Shields, Tr. 851).

65. Typically, users will perform a search using terms related to the particular file they hope to find and receive a list of possible matches. The user then chooses a file they want to download from the list. This file is then downloaded from other peers who possess that file. (CX0738 (Shields Rebuttal Expert Report ¶ 18)).

66. A document being "shared" or "made available for sharing" on a peer-to-peer network is available to be downloaded by another computer user on the same peer-to-peer network. The fact that a document is being shared, or made available for sharing, does not mean the document has been "downloaded" for viewing. (Shields, Tr. 891-892).

67. It is very difficult for a user to know what is in a document found on a peer-to-peer network without downloading and opening the document. (Wallace Tr. 1343).

68. The contents of a file that is available for sharing are not disclosed until the file is downloaded and viewed. (F. 65-67).

69. LimeWire is a peer-to-peer file-sharing application that can be used to transport files across the Internet. LimeWire is one of a number of applications that use a protocol called Gnutella (F. 70). (RX0533 (Fisk Expert Report at 9)).

70. Gnutella is a program that connects computers together in a direct peer-to-peer fashion to facilitate file sharing through searching and downloading. (RX0533 (Fisk Expert Report at 9); CX0738 (Shields Rebuttal Expert Report ¶17)).

71. A Gnutella "client" refers to the piece of software that understands the Gnutella protocol and allows a peer to interact with other peers using the Gnutella protocol. (Shields, Tr. 827).

72. In order to share a file or folder on LimeWire, the user must actively choose the file or folder to share. (RX0533 (Fisk Expert Report at 10)).

73. The 1718 File, discussed *infra* Section II.D.2., has the computer filename "insuranceaging_6.05.071.pdf". (F. 1, 78).

74. When a user makes a file available for sharing on LimeWire, LimeWire breaks apart the file names into keywords to allow other users to search for them. (RX0533 (Fisk Expert Report at 11, 13)).

75. In this case, LimeWire would break apart the "insuranceaging_6.05.071.pdf" file name into the keywords "insuranceaging" and "6.05.071" because LimeWire only recognizes the "_" as a word delimiter and does not recognize that "insuranceaging" is, in fact, the words "insurance" and "aging" merged together. (Fisk, Tr. 1154-1156; RX0533 (Fisk Expert Report at 11-12)).

76. A search for "insurance" or for "aging" would not return a search result for "insuranceaging_6.05.071.pdf". (Fisk, Tr. 1155-1156; RX0533 (Fisk Expert Report at 11-12)).

77. In order for a searcher to receive a search result for the "insuranceaging_6.05.071.pdf" file, he or she would have to enter the search terms "insuranceaging" or "6.05.071". Both of those searches are highly unusual, and it is extremely unlikely that any LimeWire user would ever enter them. (Fisk, Tr. 1155-1156; RX0533 (Fisk Expert Report at 11-12)).

2. The 1718 File

a. Background facts

78. The "1718 File" is a LabMD insurance aging report, containing 1,718 pages, dated June 2007, with the filename "insuranceaging_6.05.071.pdf". (F. 1; Joint Stipulations of Fact, JX0001-A at 1; CX0697, *in camera* (1718 File)). The peer-to-peer sharing and subsequent disclosure of the 1718 File is referred to herein as the "1718 File Incident."

79. The 1718 File was created and stored on a LabMD computer. (Daugherty, Tr. 1078-1079).

80. The 1718 File had been maintained on the LabMD computer used by LabMD's billing manager, Ms. Rosalind Woodson ("Billing Computer"). (CX0766 at 9; Daugherty, Tr. 1079).

81. The 1718 File is a billing file generated from LabMD's billing application, the Lytec system. (CX0709 (Daugherty, Dep. at 146); CX0736 (Daugherty, IHT at 83-84); CX0706 (Brown, Dep. at 23-24)).

82. The 1718 File contains the following Personal Information for approximately 9,300 consumers: names; dates of birth; nine digit numbers that appear to be Social Security numbers; CPT codes for laboratory tests conducted; and, in some instances, health insurance company names, addresses, and policy numbers. (CX0766 at 8; Answer ¶ 19; CX0697, *in camera*).

83. The CPT number is a code used for the purpose of having a standardized description of procedures or tests provided for a patient. The CPT numbers do not disclose the laboratory test performed. Determining what test was performed, as reflected by the code, requires additional research, such as going to the website for the American Medical Association or performing a Google search for the code, which is how Mr. Kam, Complaint Counsel's expert, determined the tests reflected by the CPT codes in the 1718 File. (Kam, Tr. 445-447).

84. At the time the 1718 File was downloaded by Tiversa Holding Company ("Tiversa") in February 2008 (*see* F. 121), the 1718 File was in the "My Documents" folder on LabMD's Billing Computer. (CX0710-A (Daugherty, LabMD Designee, Dep. at 200)).

85. In February 2008, the Billing Computer's "My Documents" folder was available for sharing on LimeWire. (CX0156; CX0730 (Simmons, Dep. at 12, 28-29, 32)).

86. Most of the 950 files in the "My Documents" folder on the Billing Computer that were available for sharing via LimeWire at or around the same time as the 1718 File were music or video files. (Answer ¶ 18(b); CX0154; CX0730 (Simmons, Dep. at 33-34)).

87. Eighteen documents were available for sharing in the "My Documents" folder on the Billing Computer at or around the same time as the 1718 File, three of which contained Personal Information. (Wallace, Tr. 1406-1407; RX0645 at 39, 42, 43, *in camera*).

b. LabMD discovery

88. In May 2008, Tiversa contacted LabMD and told LabMD that the 1718 File was available through LimeWire. (Answer ¶ 17; CX0766 at 8; Daugherty, Tr. 981; Joint Stipulations of Fact, JX0001-A at 4).

89. After being contacted by Tiversa in May 2008, LabMD investigated and determined that LimeWire had been downloaded and installed on the Billing Computer in 2005 or 2006. (Answer ¶ 18(a); CX0755 at 4; CX0150; CX0730 (Simmons, Dep. at 10); CX0709 (Daugherty, Dep. at 144); CX0766 at 8-9).

90. In May 2008, as part of LabMD's investigation, LabMD IT Specialist Alison Simmons inspected LabMD's computers manually to identify which computer(s) were sharing files on peer-to-peer network(s) and determined that LimeWire had been installed only on the Billing Computer. (CX0734 (Simmons, IHT at 14); CX0730 (Simmons, Dep. at 10)).

91. As part of LabMD's investigation regarding the 1718 File, Ms. Simmons took screenshots of the Billing Computer, which show the existence of LimeWire and the shared 1718 File. (CX0150; CX0151; CX0152; CX0154; CX0155; CX0156; CX0730 (Simmons, Dep. at 14-15, 21, 23-24, 27, 29, 36-37, 42, 112, 150-152)).

92. After taking the screenshots (F. 91), Ms. Simmons removed LimeWire from the Billing Computer in May 2008. (CX0730 (Simmons, Dep. at 14-15); Answer ¶ 20).

93. As part of LabMD's investigation regarding the 1718 File in May 2008, Ms. Simmons searched all computers at LabMD for file-sharing software. (CX0704 (Boyle, Dep. at 57-66, 74-88); CX0149; CX0150; CX0151; CX0152; CX0153; CX0154; CX0155; CX0156; CX0157).

94. As part of LabMD's investigation regarding the 1718 File in May 2008, Ms. Simmons did not find any file-sharing software on any LabMD computer other than the Billing Computer. (CX0730 (Simmons, Dep. at 10-11)).

95. Mr. John Boyle, LabMD's vice president of operations and general manager from November 1, 2006 until the end of August 2013, assigned Ms. Simmons, and later, IT Manager Jeffrey Martin, to search peer-to-peer networks to look for the 1718 File. (CX0704-A (Boyle, Dep. at 6-8; 63-64); CX0725-A (Martin, Dep. at 9)).

96. As part of LabMD's investigation regarding the 1718 File in May 2008, Ms. Simmons searched peer-to-peer networks from her home computer to look for the 1718 File. She searched multiple times for at least a month thereafter for the file name insuranceaging_6.05.071.pdf, partial file names, and anything with the name LabMD associated with it. (CX0730 (Simmons, Dep. at 17-18); CX0704-A (Boyle, Dep. at 63-64)).

97. As part of LabMD's investigation regarding the 1718 File, in 2013, Mr. Martin searched peer-to-peer networks for the 1718 File multiple times over the course of a few months, using the file name, and the terms "LabMD," "patient," and "aging." (CX0725-A (Martin, Dep. at 98-101); CX0704-A (Boyle, Dep. at 63-64)).

98. Through their searches (F. 96-97), Ms. Simmons and Mr. Martin were not able to find the 1718 File on any peer-to-peer networks. (CX0730 (Simmons, Dep. at 17-18); CX0725-A (Martin, Dep. at 100); CX0704-A (Boyle, Dep. at 63-64)).

99. The 1718 File was not available from LabMD's computers to be shared via any peer-to-peer networks after May 2008. (F. 92-98).

3. Tiversa

a. Tiversa's business

100. Tiversa Holding Company ("Tiversa") is a data security company that offers breach detection and remediation services. Essentially, Tiversa uses a series of algorithms to search the entire peer-to-peer network for documents of interest to its clients or potential clients, and downloads the documents that are found. (CX0703 (Boback, Tiversa Designee, Dep. at 10-12); RX0541 (Boback Trial Dep. at 19-21); Wallace Tr. 1339-1341).

101. Mr. Robert Boback is the chief executive officer of Tiversa. (CX0703 (Boback, Tiversa Designee, Dep. at 11)).

102. In July 2007, Mr. Boback hired Mr. Richard Wallace as a forensic analyst. (Wallace, Tr. 1337, 1339-1340).

103. As a forensic analyst for Tiversa, Mr. Wallace's job included writing up a narrative for clients or potential clients as to the type of information Tiversa found, where it was found, and who the disclosing source was. (Wallace, Tr. 1339-1341).

104. Mr. Wallace's job included searching peer-to-peer networks using a standard peer-to-peer Gnutella client, such as LimeWire or Kazaa, to supplement information that Tiversa's system may not have downloaded. As an example of a search, if Tiversa were looking for insurance information for a healthcare company, Mr. Wallace would conduct a search using words such as "insurance" or "report," or any word that would identify an exposed file. (Wallace Tr. 1342-1344).

105. Because it is very difficult to know what is in a document found on a peer-to-peer network without downloading and opening the document, Mr. Wallace would begin by viewing the file titles and Internet protocol ("IP") addresses[19] returned from a search. He would then download any and all information that was available from a search. (Wallace Tr. 1343-1345).

106. Tiversa maintained a depository of long servers to store data that Tiversa's searches "pulled down," or downloaded, from peer-to-peer networks, which is referred to as Tiversa's "data store" ("Data Store"). The Data Store contained copies of files that Tiversa had downloaded from the Gnutella network. The Data Store also contained information as to where the downloaded file had been located. (Wallace, Tr. 1345, 1371).

107. There are two ways for legitimate data to get into Tiversa's Data Store. Tiversa's program, Eagle Vision, will automatically download files returned from Tiversa's searches, or an analyst, such as Mr. Wallace, can insert data that the analyst has found using a stand-alone computer running a peer-to-peer client. (Wallace, Tr. 1389-1390).

108. Mr. Wallace's job as a forensic analyst included searching for exposed files on peer-to-peer networks, and recording the information disclosed, including the company that had the disclosure, and when the information was disclosed. This information would be included on a spreadsheet that Tiversa analysts would update several times a day. The purpose of the spreadsheet was so that Mr. Boback and the Tiversa sales force could make sales calls to the affected companies. (Wallace, Tr. 1437-1438).

109. When a document was downloaded by Tiversa, Tiversa would record information as to the IP address from which the document was downloaded. When contacting the affected company to sell services, Tiversa's practice was to not reveal the source of the information and to tell the potential client that the IP information had not been recorded by Tiversa. Tiversa would "strip" the IP address off the found documents and remove any metadata[20] relating to the disclosure source, while keeping a separate set of the files which included disclosure source information. (Wallace, Tr. 1344-1345, 1439-1440).

---

[19] Computers on the Internet are able to identify each other by the use of IP addresses. The IP address uniquely identifies each computer on a network. (Shields, Tr. 821-825).

[20] Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data. http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

110. When Mr. Wallace, or any other analyst at Tiversa, downloaded a file that was deemed significant, Mr. Boback would be advised, and Mr. Boback would make the decision as to how to proceed to "monetize" the file; *i.e.*, whether the information would be given to a salesperson, or whether Mr. Boback himself would contact the company, to try to sell Tiversa's services. (Wallace, Tr. 1344, 1360).

111. Tiversa would monetize information it obtained from peer-to-peer networks either by selling a monitoring contract, pursuant to which Tiversa would search for certain key words for a period of time, or by selling a "one-off" service, that would remediate just the existing disclosure problem. (Wallace, Tr. 1364).

112. A Tiversa monitoring services contract for a large financial company could cost as much as a million dollars per year, down to a few thousand dollars per month for monitoring contracts for small "mom and pop" companies. (Wallace, Tr. 1366).

113. Tiversa was having problems selling monitoring contracts, so Tiversa started contacting individual companies whose information Tiversa had discovered. Instead of a year-long monitoring contract, Tiversa could try to sell a less expensive one-time service to address the problem. This attempt to "monetize" the information through a "one-off" sale after Tiversa's discovery of information on a peer-to-peer network was known as an "incident response case," or "IRC." (Wallace, Tr. 1359-1361).

114. A hypothetical example of an IRC would be a company that had a single file exposed with 5,000 individuals' personal information, and that company would only need the name of the person exposing the file. (Wallace, Tr. 1360).

115. When a company refused to purchase Tiversa's services, Mr. Wallace observed that Mr. Boback would often respond, in reference to that company, to the effect of, "you think you have a problem now, you just wait." Thereafter, an analyst of Tiversa would input information into Tiversa's Data Store so as to make that company's information "proliferate" in Tiversa's Data Store and thereby make it appear that a file had "spread" to multiple places. Tiversa could use this Data Store "evidence" to follow up with a company to try again to get the company to purchase Tiversa's remediation services. (Wallace, Tr. 1364-1365).

116. If a potential Tiversa client would not purchase Tiversa's services, another way Tiversa would "monetize" peer-to-peer findings would be to notify an existing Tiversa client of the disclosing source of the client's information and advise the existing client to contact Tiversa's target. Tiversa could "strong-arm people that way as well." (Wallace, Tr. 1451-1452).

117. When a company refused to purchase Tiversa's services after being contacted by Tiversa about a disclosure, Tiversa would need an excuse to make contact with the company again, so it would contact the company to report that the file had proliferated, or

"spread," to additional IP addresses, including IP addresses of known "bad actors" or identity thieves. (Wallace, Tr. 1366-1368).

118. Part of Mr. Wallace's job for Tiversa was to make it appear that a company's file had spread to more IP addresses, including to IP addresses of identity thieves. He did this by placing files he might have found outside Tiversa's searching system into a folder in the Data Store and making it appear that Tiversa had located and downloaded the file from the IP address of a known bad actor. As far as the Data Store sees it, the file was downloaded from that IP address, but in reality no data transferred. (Wallace, Tr. 1367-1368).

119. Tiversa's Data Store was a record of files that were found "live" on the Internet, but also included information designed to make it appear that files had been found at other locations on the Internet. (Wallace, Tr. 1441).

120. Tiversa's Data Store is not a credible or reliable source of information as to the disclosure source or the spread of any file purportedly found by Tiversa. (F. 106-109, 115, 117-119).

b. Tiversa's dealings with LabMD

121. On or about February 25, 2008, Mr. Wallace, on behalf of Tiversa, downloaded the 1718 File from a LabMD IP address in Atlanta, Georgia, designated as 64.190.82.42. (Wallace, Tr. 1395, 1410-1411, 1440-1441; CX0307).

122. The 1718 File was found by Mr. Wallace, and was downloaded from a peer-to-peer network, using a stand-alone computer running a standard peer-to-peer client, such as LimeWire. (Wallace, Tr. 1342-1343, 1371-1372, 1440-1441).

123. After locating the 1718 File on February 25, 2008, Mr. Wallace input the information in Tiversa's Data Store. (Wallace, Tr. 1441).

124. In 2008, CIGNA Health Insurance ("CIGNA") was a company for which Tiversa was providing peer-to-peer monitoring services. An "incident record form" was prepared by Tiversa for its then-client CIGNA, and was admitted into evidence as RX0545. (Wallace, Tr. 1449-1451; RX0545).

125. Tiversa's representation to its client CIGNA, in RX0545, that the 1718 File had been found on April 18, 2008 is not correct, but was part of Tiversa's practice of ensuring that information continually flows to clients, so that it would appear that Tiversa was getting things done for the client. (Wallace, Tr. 1449-1451; RX0545 at 1).

126. Within minutes of Mr. Wallace's opening the 1718 File, Mr. Boback was viewing the document over Mr. Wallace's shoulder. Mr. Wallace observed that Mr. Boback was excited about the find. (Wallace, Tr. 1442).

127. Using the "browse host" [21] function, Mr. Wallace also downloaded 18 other LabMD documents in addition to the 1718 File, three of which contained Personal Information. (Wallace, Tr. 1372, 1400-1401, 1404-1406, 1415; *see* RX0645, *in camera* (LabMD Documents produced by Wallace at 39, 42-43)).

128. In May 2008, Tiversa began contacting LabMD to try to sell Tiversa's remediation services to LabMD. These efforts included representing to LabMD that the 1718 File had been found on a peer-to-peer network and sending LabMD a Tiversa Incident Response Services Agreement describing Tiversa's proposed fee schedule, payment terms, and services that would be provided. These contacts continued from mid-May through mid-July 2008. In these communications, Tiversa represented that Tiversa had "continued to see individuals [on peer-to-peer networks] searching for and downloading copies" of the 1718 File. (RX0050; RX0051; RX0052; RX0053; RX0054; RX0055; RX0056; RX0057; RX0058; RX0059; CX0021; *see also* Daugherty, Tr. 979-993).

129. Tiversa's representations in its communications with LabMD (F. 128) that the 1718 File was being searched for on peer-to-peer networks, and that the 1718 File had spread across peer-to-peer networks, were not true. These assertions were the "usual sales pitch" to encourage the purchase of remediation services from Tiversa. (Wallace, Tr. 1443).

130. On July 22, 2008, LabMD instructed Tiversa to direct any further communications to LabMD's lawyer. Thereafter, Tiversa ceased to press LabMD to purchase its services. (RX0059; Daugherty, Tr. 988-990).

c. Tiversa's role as source for FTC investigation

131. The FTC offered testimony concerning peer-to-peer file-sharing technology at a July 2007 hearing conducted by the House of Representatives' Committee on Oversight and Government Reform regarding peer-to-peer file-sharing technology ("2007 Congressional Hearing"). (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues)).

132. Tiversa's Mr. Boback gave testimony at the 2007 Congressional Hearing regarding peer-to-peer file-sharing technology. (Wallace Tr. 1341-1342, 1347).

133. The FTC and Tiversa began communicating approximately two months after the 2007 Congressional Hearing. These communications were as frequent as weekly during some periods. The subject matter of these communications was information available on peer-to-peer networks. (Wallace, Tr. 1346-1347, 1350).

[21] "Browse host" is the ability for one LimeWire user to view all the files another LimeWire user has made available to share. (RX0533 (Fisk Expert Report at 16)).

134. In the fall or winter of 2007, representatives of the FTC visited Tiversa's facility in Pennsylvania. Following that meeting, the FTC began requesting that Tiversa provide information to the FTC. (Wallace, Tr. 1350-1351).

135. Tiversa did not want the FTC to issue a formal request for information, such as a Civil Investigative Demand ("CID"), directly to Tiversa because Tiversa had been in talks regarding a possible acquisition and Mr. Boback did not want Tiversa to be "in the middle of a civil investigative demand." Mr. Boback wanted the CID to be issued to a third party to "separate" the CID from Tiversa, "to try to create some distance" from Tiversa. (CX0703 (Boback, Dep. at 142-143); Wallace, Tr. 1351-1353, 1362).

136. The Privacy Institute was created for the purpose of receiving the CID from the FTC. The Privacy Institute did not exist previously. (RX0541 (Boback Trial Dep. at 38-40; 42-44); Wallace, Tr. 1353).

137. In 2009, in order to obtain Tiversa's information and documents, the FTC issued a CID to The Privacy Institute ("FTC CID"), and not to Tiversa, which was the actual target of the CID. (Kaufman, Tr. 1114; RX0525 (Kaufman, Dep. at 11-20) ("There was a request from Tiversa that we issue the CID to The Privacy Institute, and that is the entity that received the CID from the FTC.").

138. In response to the FTC CID to The Privacy Institute (F. 137), the FTC received the 1718 File and other evidence that "is germane to th[is] case." (CX0697 (*in camera*); Kaufman, Tr. 1114; RX0525 (Kaufman, Dep. at 11-20); *see also* RX0526 (Complaint Counsel's Amended Response to LabMD, Inc.'s First Set of Requests for Admission, Response No. 20 (admitting that as part of Complaint Counsel's Part II investigation of LabMD, the FTC issued a CID to The Privacy Institute and received the 1718 File)).

139. Mr. Wallace assisted in responding to the FTC CID (F. 137) by composing a spreadsheet of names of companies whose information exposure met a threshold of exposing 100 individuals' personal information. He also collected the associated files, which were burned to a computer disc. (Wallace, Tr. 1353-1354).

140. The spreadsheet provided in response to the FTC CID (F. 137) was derived from Tiversa's list of IRC's, *i.e.*, companies that Tiversa had targeted to try to sell Tiversa's remediation services. (F. 113; Wallace, Tr. 1358-1359, 1452-1453; *see* CX0307).

141. Mr. Boback directed Mr. Wallace to "make sure [LabMD is] at the top of the list" being provided to the FTC pursuant to the FTC CID. (Wallace, Tr. 1365).

142. The list of names Tiversa provided to the FTC in response to the FTC CID (F. 137) includes LabMD and identifies LabMD as the "data owner/leaker" of a file identified as "insuranceaging_6.05.071.pdf". (CX0307; Wallace, Tr. 1394).

143. The list of names Tiversa provided to the FTC in response to the FTC CID (F. 137) contained names that did not meet the 100 person exposure threshold described in F. 139.

These names were placed on the list at Mr. Boback's direction in order to get Tiversa "more bang for the buck," *i.e.*, in the hope that once the company was contacted by the FTC, the company would then buy Tiversa's services out of fear of an enforcement action. (Wallace, Tr. 1362-1363).

144. The list of names provided by Tiversa to the FTC in response to the FTC CID (F. 137), at Mr. Boback's direction, was "scrubbed" of names of existing or prospective Tiversa clients that otherwise met the 100 person exposure threshold. (Wallace, Tr. 1363-1364).

145. In the fall of 2009, representatives of Tiversa, including Mr. Wallace and Mr. Boback, met with FTC staff, including a member of Complaint Counsel's trial team in this case, to discuss Tiversa's response to the FTC CID (F. 137). (Wallace, Tr. 1385-1386, 1452).

d. CX0019

146. On the return trip from Tiversa's meeting with FTC staff in 2009 (F. 145), based on statements of Mr. Boback, Mr. Wallace understood that Tiversa needed to increase the apparent "spread" of the files identified on the list provided to the FTC pursuant to the FTC CID; that Mr. Wallace was to search for the files again to see if they are available at other IP addresses in addition to the address provided on the list; and that if the files were not, in fact, available at any additional IP addresses, Mr. Wallace was to make it appear that the files were available at additional IP addresses. (Wallace, Tr. 1386-1388).

147. After Tiversa's meeting with FTC staff in 2009 (F. 145), Mr. Wallace searched Tiversa's Data Store to see if the LabMD insurance aging file had been "picked up" from the automatic searches being performed by Tiversa for its healthcare clients, and he determined that it had not been. (Wallace, Tr. 1388-1390).

148. CX0019 purports to show that Tiversa had downloaded the 1718 File from four IP addresses on particular dates and times. Mr. Wallace created CX0019, at Mr. Boback's direction, in 2013, near the time of Boback's deposition, to make it appear that the 1718 File had "spread" to IP addresses belonging to known identity thieves, and that the 1718 File had not been found at an Atlanta IP address, when, in fact, none of this is true. Mr. Boback specifically asked Mr. Wallace to include a San Diego IP address. (Wallace, Tr. 1368-1370, 1381, 1446-1447).

149. Although it was not true, Mr. Wallace included on CX0019 the IP address 173.16.83.112 as one of the IP addresses where the 1718 File had been found because that IP address belonged to an individual in Apache Junction, Arizona that Wallace believed to be an identity thief, based on data in Tiversa's Data Store indicating that the individual at that address possessed over 3,000 tax returns that he appeared to be selling. (Wallace, Tr. 1376-1377).

150. In order to appear to be providing a client with valuable information, Tiversa would create the appearance of a "spread" of a client's file. (F. 115, 117-119; Wallace, Tr. 1391).

151. It was common practice for Tiversa to create documents such as CX0019 to make it appear that a file had "spread" to various IP addresses. (Wallace, Tr. 1368-1369, 1390-1391).

152. Tiversa had approximately 20 IP addresses that it would use when making it appear as if files had been spread across the Internet, including to identity thieves. Some IP addresses were used more frequently than others. For example, Tiversa knew of IP addresses that had gone "dead" after law enforcement took action. If Tiversa claimed the 1718 File was found at one of these long-gone addresses, such as the IP address at Apache Junction (F.149), there would be no way to contradict Tiversa's claim. (Wallace, Tr. 1376-1377, 1445).

153. The 1718 File was never found at any of the four IP addresses listed on CX0019. (Wallace, Tr. 1370, 1383-1384).

154. To Mr. Wallace's knowledge, the originating disclosing source in Atlanta is the only location at which the 1718 File was ever located. (Wallace, Tr. 1443-1444).

4. Credibility Findings Concerning the 1718 File Incident

155. Based on Mr. Wallace's forthrightness in response to questioning, and his overall demeanor observed during his questioning, Mr. Wallace is a credible witness.

156. Tiversa "has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations." (Dissenting Statement of Commissioner J. Thomas Rosch re FTC File No. 1023099 (June 21, 2012) at 1, *at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./1023099-labmd-full-commission-review-jtr-dissent.pdf; *see also e.g.*, F. 100, 108-114, 121, 126, 128).

157. Mr. Boback was motivated to retaliate against LabMD for LabMD's refusal to purchase remediation services from Tiversa, including by making the disclosure of the 1718 File appear widespread and dangerous. (F. 115-118, 126, 128-130, 148-154).

158. Mr. Boback's motive to retaliate against LabMD for refusing to purchase remediation services from Tiversa (F. 157) resulted in Tiversa's decision to include LabMD in the information provided to the FTC in response to the FTC CID (F. 137) and in the creation of CX0019. (F. 141-144, 146-149).

159. CX0019 is not credible or reliable evidence to show that the 1718 File spread on any peer-to-peer network. (F. 156-158).

160. Because of Mr. Boback's biased motive, Mr. Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of Respondent. (F. 156-159).

161. Mr. Boback has previously asserted that Tiversa found other files that it had not found. (F. 162-163).

162. Mr. Wallace helped Mr. Boback prepare for his testimony before the 2007 Congressional Hearing by giving Boback documents that Wallace had found on the Internet via peer-to-peer sharing from a time period that was before Tiversa had hired Wallace. Mr. Boback testified at the 2007 Congressional Hearing that Tiversa's system had found those documents, when in fact, Mr. Wallace, and not Tiversa or someone using Tiversa's system, had done so. (Wallace, Tr. 1432-1434).

163. There were "multiple times" when Mr. Boback would make statements that a company's documents had spread all over the Internet and then create the appearance that information was found in locations where it never existed. (Wallace, Tr. 1453-1454, 1457-1458) (testifying to a highly publicized instance as one example).

164. In 2014, the Chairman of the United States House Oversight and Government Affairs Committee ("OGR") commenced an investigation of Tiversa regarding its involvement with government agencies. The investigation continued over a period of months and included investigation into Tiversa's relationship with the FTC. (JX0003; RX0542 (June 11, 2014 OGR Letter from Issa to Ramirez); RX0543 (December 1, 2014 OGR Letter from Issa to Ramirez)).

165. The OGR staff report regarding the investigation referred in F. 164 concluded, *inter alia*, that Tiversa and Mr. Boback provided incomplete, inconsistent, and/or conflicting information to the FTC in this matter. (RX0644).

166. Having observed Mr. Boback's June 7, 2014 video deposition (RX0541 (Boback Trial Dep.); Tr. 1268-1269), taken by Respondent for purposes of trial testimony, Mr. Boback was evasive and lacked forthrightness in response to questioning.

167. Based on F. 155-166, and observation of Mr. Boback's overall demeanor during the June 7, 2014 video deposition (RX0541 (Boback Trial Dep.)), Mr. Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of Respondent.

168. Mr. Wallace's testimony, including without limitation regarding CX0019, is credited over any contrary testimony or other evidence provided by Boback or Tiversa. (F. 155-167).

5. Professor Eric Johnson

169. In February 2009, Professor Eric Johnson, while with Dartmouth College ("Dartmouth"), authored an article titled, "Data Hemorrhages in the Health-Care Sector." The article addresses data breaches and inadvertent disclosures of information by healthcare providers (the "Johnson Article"). (CX0382; Johnson, Tr. 753, 757).

170. Tiversa was a research partner for the Johnson Article, and assisted Professor Johnson in his research for the Johnson Article. (Johnson, Tr. 753-755).

171. The Johnson Article represents that the 1718 File was found as a result of Professor Johnson's research. (CX0382 at 11).

172. Tiversa's role in the research was to conduct searches for Professor Johnson and to forward files to him for further analysis. All the files examined in Professor Johnson's research for the Johnson Article were provided to him by Tiversa. (Johnson, Tr. 758-759, 793-794).

173. The first phase of the research, conducted in the first two weeks of January 2008, used a set of search terms, or "digital signature," related to the top ten publicly traded healthcare companies, as well as "generic" healthcare-related terms. The first phase of Professor Johnson's research did not uncover the 1718 File. (Johnson, Tr. 758-759, 765-766, 776-777, 780).

174. The second phase of Professor Johnson's research took place over a six-month period in the spring of 2008. It was Professor Johnson's "understanding" that files provided by Tiversa in the second phase of the research were files that Tiversa discovered by searching "host" locations found in the first phase of the research, or were files that Tiversa had otherwise discovered on its own. (Johnson, Tr. 762-763).

175. Although Professor Johnson understood that Tiversa had found the 1718 File, he had no knowledge of what search term was used to find the 1718 File. (Johnson, Tr. 764-765).

176. Tiversa employee Mr. Chris Gormley was Professor Johnson's main contact at Tiversa to discuss the research and progress of the Johnson Article. (Johnson, Tr. 770-771).

177. In an email to Mr. Gormley dated April 29, 2008, Professor Johnson stated that it was going "well on the medical files. We are working on the report right now. We turned up some interesting stuff – not as rich as the banks, but I guess that could be expected. Any chance you could share a couple of your recent medical finds that we could use to spice up the report? You told me about the one database you found that could really boost the impact of the report." (RX0483 at 1-2).

178. The 1718 File was one of many files that Tiversa provided to Professor Johnson. Despite persistent questioning, Professor Johnson did not provide a clear response as to: (1) whether Tiversa provided the 1718 File as a product of Professor Johnson's research parameters, including the "host" browsing second phase of Professor Johnson's research, as asserted in the Johnson Article; or (2) whether Tiversa provided the 1718 File in response to Professor Johnson's April 2008 request (F. 177) that Tiversa provide a "recent medical find" to "spice up" the Johnson Article. (Johnson, Tr. 774-777, 779-780; CX0382 at 11 (stating that the 1718 File was discovered in the second phase through

examining shared files on hosts where other "dangerous" data had been found); CX0483 at 2).

179. While Professor Johnson was confident that the 1718 File was not found in the first phase of his research, Professor Johnson either does not know, or was unwilling to say, whether the 1718 File was discovered as a result of his search protocol for the second phase of the research, notwithstanding the contrary representation in the Johnson Article. (*See* F. 173-175, 178; Johnson, Tr. 777-780).

180. An FTC attorney contacted Professor Johnson in February 2009, and asked for a copy of the Johnson Article, and Professor Johnson complied by sending a copy. (RX0403; Johnson, Tr. 784).

181. Professor Johnson did not provide the 1718 File to the FTC, and did not share files containing sensitive information with anyone. (Johnson, Tr. 785, 794).

E. THE SACRAMENTO INCIDENT

1. Sacramento Police Department's Discovery of LabMD Documents

182. On October 5, 2012, the Sacramento California Police Department (the "SPD") found 40 LabMD "day sheets," (F. 199) (hereafter, the "Day Sheets"), 9 copied checks, and 1 money order made payable to LabMD in a house in Sacramento, California (collectively, the "Sacramento Documents"). (Joint Stipulations of Fact, JX0001-A at 4; CX0087, *in camera* (LabMD Day Sheets); CX0088, *in camera* (LabMD Copied Checks at 1-10); CX0720 (Jestes, Dep. at 17-18, 22-23, 33-37)). This event is referred to herein as the "Sacramento Incident."

183. The Day Sheets found by the SPD on October 5, 2012 contain the following Personal Information of approximately 600 consumers: names and nine digit chart numbers that appear to be SSNs. (CX0720 (Jestes, Dep. at 35-37); CX0087, *in camera* (LabMD Day Sheets); RRCCFF 1724).

184. The dates of the Day Sheets contained in CX0087 range from June 2007 to March 2009, with 28 from various months in the year 2008, 10 from various months in 2007, and 2 from March 2009. (CX0087, *in camera* (LabMD Day Sheets)).

185. The nine copied checks found by the SPD on October 5, 2012 contain the following Personal Information of nine consumers: names, addresses (for all but one), and bank account numbers. The money order does not contain any Personal Information. (CX0088 *in camera*, (LabMD Copied Checks at 1-10)).

186. The dates of the nine copied checks found by the SPD on October 5, 2012 range from May 2007 to March 2009. (CX0088, *in camera* (LabMD Copied Checks at 1-9) (4 checks from 2007; 4 checks from 2008; 1 check from 2009)).

187. The date of the one money order found by the SPD on October 5, 2012 is August 21, 2008. (CX0088, *in camera* (LabMD Copied Checks at 10)).

188. Detective Karina Jestes of the SPD participated in an investigation of 5661 Wilkinson Street in Sacramento, California ("5661 Wilkinson"), initiated on October 5, 2012, along with three other officers. (CX0720 (Jestes, Dep. at 17-18)).

189. The SPD investigation concerned a woman whose utility bill had been compromised and who was then receiving an additional utility bill for an address at 5661 Wilkinson, to which she had no connection. (CX0720 (Jestes, Dep. at 17-18)).

190. Detective Jestes went to 5661 Wilkinson, entered the property, and executed a search. (CX0720 (Jestes, Dep. at 17-19)).

191. Detective Jestes concluded that the search of 5661 Wilkinson revealed evidence of utility billing theft, evidence that the occupants of the home were using someone else's name for the gas utility bill, narcotics paraphernalia, narcotics, and several additional items that, Detective Jestes believed, showed that identity theft was occurring at the house. (CX0720 (Jestes Dep. at 19-20)).

192. The search of 5661 Wilkinson also uncovered the Sacramento Documents, described in F. 182-187. (Joint Stipulations of Fact, JX0001-A at 4; CX0720 (Jestes, Dep. at 23)).

193. On October 5, 2012, Mr. Erick Garcia and Ms. Josie Maldonado were arrested and charged with identity theft, receiving stolen property, possession of methamphetamine, and the possession of narcotics paraphernalia. (CX0720 (Jestes, Dep. at 25)).

194. Mr. Garcia and Ms. Maldonado pled *nolo contendere* to identity theft and were sentenced to probation and a sheriff's work project. (CX0720 (Jestes, Dep. at 43-45)).

195. The Day Sheets found by the SPD during the search of 5661 Wilkinson on October 5, 2012 were seized by the SPD and booked into evidence. (CX0720 (Jestes, Dep. at 30-31)).

196. The copies of checks and the canceled money order found by the SPD during the search of 5661 Wilkinson on October 5, 2012 were seized by the SPD and booked into evidence. (CX0720 (Jestes, Dep. at 31-32)).

2. Connection between the Sacramento Documents and LabMD's Computer Network

197. The Sacramento Documents were found in paper form, not in electronic form. (CX0720 (Jestes, Dep. at 58)).

198. As part of its consumer billing process, LabMD produced reports called day sheet transaction detail reports, referred to as "day sheets." (CX0715-A (Gilbreth, Dep. at 42); *see, e.g.*, CX0087, *in camera*).

199. Day sheets are reports that were created, accessed, and printed electronically through LabMD's billing application, Lytec, to ensure payment had been received and posted. (CX0733 (Boyle, IHT at 33); CX0715-A (Gilbreth, Dep. at 42); CX0714-A ([Former LabMD Employee], Dep. at 59-60)).

200. LabMD's billing department used computers to create day sheets of payments received from consumers, which may include consumers' names; SSNs; and methods, amounts, and dates of payments. (Answer ¶ 9(b); CX0715-A (Gilbreth, Dep. at 37-38, 46-49)).

201. Day sheets could include billing date; provider number; place of service; diagnosis code, which is a standardized code that identifies the symptoms leading to the procedure being performed; payment code; payment amount; charges; credits; and adjustments. (CX0714-A ([Former LabMD Employee], Dep. at 62-63); CX0715-A (Gilbreth, Dep. at 48-49); *e.g.*, CX0087, *in camera*).

202. Copies of patient checks were attached to day sheets. (CX0715-A (Gilbreth, Dep. at 50-51)).

203. Day sheets were created electronically but were not saved electronically. Day sheets were then printed almost every day. Once the day sheets were printed, "there is no electronic record in the system." (CX0733 (Boyle, IHT at 37-38); CX0715-A (Gilbreth, Dep. at 43); CX0714-A ([Former LabMD Employee], Dep. at 59-60)).

204. The printed day sheets were made part of batch reports. If a batch report did not balance, then the day sheet was shredded and a new day sheet was created. Only balanced day sheets were retained. (CX0714-A ([Former LabMD Employee]), Dep. at 61-62).

205. Day sheets could be printed by any of LabMD's billing employees who posted payments or by a LabMD billing manager. (CX0715-A (Gilbreth, Dep. at 42); CX0714-A ([Former LabMD Employee], Dep. at 64-65)).

206. Day sheets were stored in paper files at LabMD. (CX0733 (Boyle, IHT at 33-39); CX0710-A (Daugherty, LabMD Designee, Dep. at 60); CX0715-A (Gilbreth, Dep. at 43-45); CX0714-A ([Former LabMD Employee], Dep. at 58-61)).

207. After day sheets were generated by LabMD through the Lytec system, although LabMD billing employees had the option to save or to print off day sheets, LabMD billing employees did not save them. (CX0714-A ([Former LabMD Employee], Dep. at 60-61 ("I don't know of anyone who actually saved them. . . . "I never saved [them].")); CX0715-A (Gilbreth, Dep. at 43 (day sheet reports were not created in an electronic format such as an electronic file)).

208. Beginning in or around January 2013, LabMD began to electronically scan some of its documents for a medical records archiving project. This project began with archiving old insurance documents, such as Explanation of Benefits documents. The archiving project, which was ongoing, has also included scanning of some retained day sheet printouts and check copies. (CX0716 (Harris Dep. at 25-26); CX0733 (Boyle, IHT at 37, 46-47)).

3. Follow up to Discovery of the Sacramento Documents

209. After finding the Sacramento Documents, Detective Jestes performed an Internet search and learned that the FTC was investigating LabMD. Approximately one week after the October 5, 2012 discovery of the Sacramento Documents, Detective Jestes contacted the FTC regarding the Sacramento Documents. (CX0720 (Jestes, Dep. at 60-62)).

210. In December 2012, the SPD provided the Sacramento Documents to the FTC. The SPD made the determination not to return the Sacramento Documents to LabMD based on the FTC's investigation of LabMD. (CX0720 (Jestes, Dep. at 60-61)).

211. On January 30, 2013, the FTC notified LabMD that the FTC had the Sacramento Documents. (CX0227; Daughtery, Tr. 1013-1014).

212. On March 27 or 28, 2013, LabMD sent 682 letters to the consumers named in the Sacramento Documents notifying them of the Sacramento Incident, describing steps such as registering a fraud alert with credit bureaus, offering one year of free credit monitoring services, and inviting consumers to contact LabMD with questions or concerns. (CX0710-A (Daugherty, LabMD Designee, Dep. at 63, 68-69); CX0709 (Daugherty, Dep. at 120); CX0227).

4. Lack of Foundation for Admission of CX0451

213. Mr. Kevin Wilmer is an investigator with the FTC. (Wilmer, Tr. 331).

214. CLEAR (Consolidated Lead Evaluation and Reporting) is an investigative software database program, provided by Thompson Reuters Corporation (Thompson Reuters), that is used by investigators at the FTC to obtain information on individuals and corporations. Mr. Wilmer's "understanding," based on his training and experience with the CLEAR database, is that the information contained in the CLEAR database is an aggregation of information obtained from a variety of sources, including credit bureau information, utility information, information from civil judgments and criminal convictions, and other forms of publicly and privately available information. (Wilmer, Tr. 335, 359, 362, 364).

215. Mr. Wilmer was provided with an electronic copy of CX0085, which he was told consisted of copies of the Sacramento Documents (F. 182). (Wilmer, Tr. 338-339).

216. The first four pages of CX0085 are copies of the checks and a canceled money order found by the SPD during the search of 5661 Wilkinson on October 5, 2012 that comprise CX0088. Pages 5 through 44 of CX0085 are copies of the Day Sheets found by the SPD

during the search of 5661 Wilkinson on October 5, 2012 that comprise CX0087. (CX0085, *in camera* (LabMD Day Sheets and Copied Checks).

217. Mr. Wilmer concluded, but did not confirm, that the nine digit numbers in pages 5 through 44 of CX0085 represented Social Security numbers. (Wilmer, Tr. 340).

218. Mr. Wilmer was asked by Complaint Counsel to determine whether Social Security numbers in pages 5 through 44 of CX0085 had been used by people with different names. He was not asked to confirm that the nine digit numbers appearing on CX0085 are Social Security numbers corresponding to the names that are listed on CX0085. (Wilmer, Tr. 341-342).

219. To perform the task set forth in F. 218, Mr. Wilmer issued a "query" to the CLEAR database. Specifically, Mr. Wilmer copied each number that he believed to be a Social Security number from CX0085 and pasted the number onto a CLEAR-provided spreadsheet. He then submitted the spreadsheet with a request that CLEAR use its "batching" function to query the CLEAR database to determine who used that apparent Social Security number and return the information to him. (Wilmer, Tr. 342-345, 359-360).

220. In response to Mr. Wilmer's CLEAR database query, described in F. 219, CLEAR returned a spreadsheet containing the nine digit numbers that Mr. Wilmer had entered, and CLEAR's data, drawn from its various sources, as to the names of people who used those numbers. The CLEAR spreadsheet also provided in some instances a date of birth, date of death, gender, home address and the first or last time a number was used. (Wilmer, Tr. 345-346, 361, 364).

221. Mr. Wilmer identified a document, marked for identification as CX0451, as the results returned to him by Thompson Reuters in response to his CLEAR database query, to which Mr. Wilmer added certain color coding to differentiate various names. (Wilmer, Tr. 350, 359).

222. Mr. Wilmer does not know whether the nine digit numbers he copied from CX0085 and entered into his CLEAR database query as apparent Social Security numbers actually belonged to the associated names on CX0085. (Wilmer, Tr. 358).

223. CX0451 does not indicate which individual associated with a Social Security number is the true owner of the number, if any. CLEAR only indicates that an individual is associated with a Social Security number. (Wilmer, Tr. 363-364).

224. Mr. Wilmer did not ask CLEAR to identify the source(s) of the data that CLEAR used to populate the CLEAR spreadsheet, although he could have received this information if he asked, because that was not part of his assignment. (Wilmer, Tr. 365).

225. Mr. Wilmer does not know, and did not ask CLEAR, whether any of the numbers reported by CLEAR as a Social Security number associated with an individual had

stemmed from bad keystrokes on the part of a reporting source such as a bank. (Wilmer, Tr. 366).

226. Mr. Wilmer does not know if some of the people listed on CX0085 had knowingly and willingly shared their personal information for others to use, or whether they had family members who may have taken their personal information without consent. Mr. Wilmer was not asked to determine these matters, and was not asked to and did not contact any of the individuals listed on CX0085. (Wilmer, Tr. 367-369).

227. Based on the failure to demonstrate the authenticity or reliability of the data returned by the CLEAR database, which is contained in proffered CX0451, the document cannot properly support any factual finding or any valid conclusion in this case. (*See* F. 217-226).

F. IDENTITY THEFT HARM

228. "Identity theft" refers to the use of another person's identity without his or her permission. This includes using another person's personal identifiers to impersonate that person. (CX0742 (Kam Expert Report at 10); Kam, Tr. 394).

229. "Identity fraud" refers to the unauthorized use of another person's information to achieve illicit financial gain. Types of identity fraud are "new account fraud," "existing non-card fraud," and "existing card fraud." (CX0742 (Kam Expert Report at 10); CX0741 (Van Dyke Expert Report at 3)).

230. "New account fraud" ("NAF") is identity fraud perpetrated through the use of another person's personally identifiable information to open new, fraudulent accounts. (CX0741 (Van Dyke Expert Report at 3)).

231. "Existing non-card fraud" ("ENCF") is identity fraud perpetrated through the use of existing checking or savings accounts or existing loans, insurance, telephone, and utilities accounts. (CX0741 (Van Dyke Expert Report at 3)).

232. "Existing card fraud" ("ECF") is identity fraud perpetrated through use of existing credit or debit cards and/or their account numbers. (CX0741 (Van Dyke Expert Report at 3)).

233. "Medical identity theft," also known as "medical identity fraud," is the unauthorized use of a third party's personally identifiable information to obtain medical products or services, including but not limited to: office visits and consultations, medical operations, and prescriptions. Medical identity theft may also include attempts to fraudulently bill health insurance providers. (CX0741 (Van Dyke Expert Report at 3); CX0742 (Kam Expert Report at 11-12); Kam, Tr. 395).

234. A "data breach" refers to the unauthorized disclosure of personally identifying information. (Van Dyke, Tr. 589; Kam, Tr. 378).

235. As a matter of common usage, the generic term "identity theft" may include "identity fraud" (with its subsets, NAF, ENCF, ECF, and medical identity theft). (Van Dyke, Tr. 577-579; CX0741 (Van Dyke Expert Report at 3)).

236. Identity theft and identity fraud are distinguishable from a "data breach," in that a data breach refers only to the unauthorized exposure of personal information, while identity theft and identity fraud refer to the improper use of personal information. (F. 228-229, 234).

237. Complaint Counsel's proffered expert on computer security, Dr. Raquel Hill (F. 4-5), acknowledged that she did not have an opinion with regard to the likelihood of consumer harm. Dr. Hill was instructed to "assume" that identity theft harm could occur if the information contained on LabMD's network was exposed. Dr. Hill further assumed, in assuming such harm could occur, that such harm was likely. (Hill, Tr. 216-219; CX0740 (Hill Expert Report at 20 ¶ 49)).

238. Complaint Counsel's proffered expert on the likelihood of consumer harm in this case, Mr. Rick Kam (F. 9-11) used the following four factors to examine "the likely risk of harm to consumers from unauthorized disclosure" of Personal Information: (1) the nature and extent of the sensitive Personal Information exposed; (2) the unauthorized person who obtained information or to whom the disclosure was made, to determine whether the person possessing the information presents a low risk of misuse, or a higher risk of misuse, such as an identity thief; (3) whether the sensitive Personal Information was actually acquired or viewed; and (4) the extent to which the risk from the exposure has been mitigated, including whether or not "the data is still available for others to misuse." (Kam, Tr. 404-406; CX0742 (Kam Expert Report at 17-18)).

239. Mr. Kam applied the four factor risk assessment test referenced in F. 238 to determine the likelihood of harm from the exposure of the 1718 File. (CX0742 (Kam Expert Report at 18-19)).

240. In applying the second and third factors of the four factor risk assessment test (F. 238) to determine the likelihood of identity theft harm from the disclosure of the 1718 File, Mr. Kam relied upon the discredited deposition testimony of Mr. Boback (F. 167) that the 1718 File was found at four IP addresses, along with unrelated sensitive consumer information that could be used to commit identity theft, and that law enforcement had apprehended someone suspected of identity theft of fraud using one of those IP addresses. (CX0742 (Kam Expert Report at 19); Kam, Tr. 409-410).

241. In applying the second and third factors of the four factor risk assessment test (F. 238) to determine the likelihood of identity theft harm from the disclosure of the 1718 File, Mr. Kam relied upon the discredited deposition testimony of Mr. Boback (F. 167) that the 1718 File had been found at four IP addresses on four different dates and had also been found by Tiversa just before Mr. Boback provided deposition testimony in November 2013. (CX0742 (Kam Expert Report at 19); Kam, Tr. 409-410).

242. In Mr. Kam's experience, in every data breach, some victim has come forward. Mr. Kam acknowledged that no evidence has been presented of any individual listed in the Sacramento Documents or in the 1718 File having come forward to report identity theft harm. (Kam, Tr. 532-533).

243. Mr. Kam was unaware of any actual victims of identity theft or fraud of any individuals listed on the 1718 File. (Kam, Tr. 507).

244. For the purposes of his analysis, Mr. Kam "assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks." (CX0742 (Kam Expert Report at 5)).

245. Mr. Kam is not an expert in computer network security and did not analyze any of LabMD's specific practices with respect to LabMD's computer networks or assess the probability that LabMD's computer networks will be breached in the future. (Kam, Tr. 518).

246. Mr. Kam based his opinion on the likelihood of medical identity theft harm primarily on the 2013 Survey on Medical Identity Theft by Ponemon Institute ("2013 Ponemon Survey"). (CX0742 (Kam Expert Report at 15, 19-20); Kam, Tr. 423).

247. The 2013 Ponemon Survey, conducted in September 2013, had a response rate of only 1.8 %, which the 2013 Ponemon Survey acknowledged, and which, Mr. Kam agreed, creates a non-response bias, *i.e.*, a failure to take into account that those who were surveyed but did not respond might have a different answer to the question. (Kam, Tr. 540-541; RX0528 (2013 Ponemon Survey at 31)).

248. The 2013 Ponemon Survey's sampling frame (the source from which a sample is drawn) contained individuals who were prescreened from a larger sample on the basis of their identity theft or identity fraud experience. The 2013 Ponemon Survey acknowledged, and Mr. Kam agreed, that this resulted in a sampling frame bias. (RX0528 (2013 Ponemon Survey at 28, 32); Kam, Tr. 541).

249. The 2013 Ponemon Survey compensated respondents to complete the survey within a set period of time, which the 2013 Ponemon Survey acknowledged was an inherent limitation to its survey research. (RX0528 (2013 Ponemon Survey at 32); *see also* Kam, Tr. 541).

250. The 2013 Ponemon Survey stated: "[m]any cases of medical identity theft reported in this study result from the sharing of personal identification with family and friends. In some cases, family members take the victim's personal credentials without consent. Rarely does it occur from data breaches, malicious insiders, an identity thief or loss of medical credentials." (RX0528 (2013 Ponemon Survey at 27)).

251. Mr. Kam acknowledged that medical identity theft rarely occurs from data breaches or the acts of an identity thief and acknowledged that most occurrences of medical identity

theft were from someone knowingly sharing their personal information or medical credentials and from instances where a family member took another family member's personal information or medical credentials without consent. (Kam, Tr. 486-487).

252. Complaint Counsel's second proffered expert on the likelihood of consumer harm in this case, Mr. James Van Dyke (F. 12-15) based his analysis principally on identity theft statistics derived from the Javelin 2013 Identity Fraud Survey ("2013 Javelin Survey"). The 2013 Javelin Survey was conducted in October 2013 among 5,634 adults in the United States. Javelin's 2014 Identity Fraud Report ("2014 Javelin Report") is based on the results of the 2013 Javelin Identity Fraud Survey. The Javelin Identity Theft Survey is conducted annually. (CX0741 (Van Dyke Expert Report at 2-4, and Attachment 1); Van Dyke, Tr. 583, 602-604).

253. Mr. Van Dyke selected the 2013 Javelin Survey and 2014 Javelin Report to support his opinions and calculations of likely identity theft harm from the exposure of the 1718 File because of the discredited deposition testimony of Mr. Boback in November 2013 (F. 167) that Tiversa had located the 1718 File on peer-to-peer networks on IP addresses from four locations other than LabMD. (CX0741 (Van Dyke Expert Report at 6-8); Van Dyke, Tr. 668-669).

254. In connection with Javelin Research, Mr. Van Dyke has occasionally been provided with a list of names and asked to conduct a survey from among those individuals. (Van Dyke, Tr. 730).

255. Mr. Van Dyke did not conduct a survey of the 9,300 consumers listed on the 1718 File. (Van Dyke, Tr. 690, 726; *see also* CX0741 (Van Dyke Expert Report)).

256. Mr. Van Dyke did not conduct a survey of the 600 consumers listed in the Sacramento Documents. (*See* Van Dyke, Tr. 574-741; CX0741 (Van Dyke Expert Report)).

257. For the purposes of his analysis, Mr. Van Dyke "assumed that LabMD failed to provide reasonable and appropriate security for the personally identifiable information maintained on its computer networks" and that, therefore, all individuals whose information is maintained on LabMD's computer network are "at risk" of "exposure to a likelihood" of identity fraud and medical identity fraud. Mr. Van Dyke did not do any independent analysis of LabMD's network security. (CX0741 (Van Dyke Expert Report at 2, 13); Van Dyke, Tr. 695-696).

258. Mr. Van Dyke did not, and was unable to, provide any quantification of the risk of identity theft harm for the 750,000 consumers whose personally identifiable information is maintained on LabMD's computer networks, because he did not have evidence of any data exposure with respect to those individuals, except as to those that were listed on the 1718 File or in the Sacramento Documents. (Van Dyke, Tr. 631; *see also* Van Dyke, Tr. 610).

III. ANALYSIS

A. BURDEN OF PROOF

The parties' burdens of proof are governed by Rule 3.43(a) of the Federal Trade Commission's ("FTC" or "Commission") Rules of Practice for Adjudicative Proceedings ("Rules"), Section 556(d) of the Administrative Procedure Act ("APA"), and case law. Pursuant to Commission Rule 3.43(a), "[c]ounsel representing the Commission . . . shall have the burden of proof, but the proponent of any factual proposition shall be required to sustain the burden of proof with respect thereto." 16 C.F.R. § 3.43(a). Under the APA, "[e]xcept as otherwise provided by statute, the proponent of a rule or order has the burden of proof." 5 U.S.C. § 556(d).

It is well established that the preponderance of the evidence standard governs FTC enforcement actions. *In re Rambus, Inc.*, 2006 FTC LEXIS 101, at *45 (Aug. 20, 2006); *In re POM Wonderful LLC*, 2012 FTC LEXIS 106, at *463-65 (May 17, 2012) (initial decision); *In re Adventist Health System/West*, 117 F.T.C. 224, 1994 FTC LEXIS 54, at *28 (Apr. 1, 1994) ("Each element of the case must be established by a preponderance of the evidence . . ."). The Supreme Court has held that Section 7(c) of the APA, which is applicable to administrative adjudicatory proceedings unless otherwise provided by statute, establishes "a standard of proof and . . . the standard adopted is the traditional preponderance-of-the evidence standard." *Steadman v. SEC*, 450 U.S. 91, 95-102 (1981).

Section 5(n) of the Federal Trade Commission Act ("FTC Act") requires that FTC Complaint Counsel ("Complaint Counsel") prove, *inter alia*, that challenged conduct "causes or is *likely to cause* substantial injury to consumers." 15 U.S.C. § 45(n) (emphasis added). Respondent argues that, because Section 5(n) uses the phrase "likely to cause," Complaint Counsel has the burden of proving the likelihood of substantial consumer injury in this case by clear and convincing evidence. This argument contradicts clearly established law, stated above, and Respondent's own stipulations in this case. *See* Joint Stipulations of Fact, JX0001-A at 2-3 ("The standard of proof is preponderance of the evidence."). None of the authorities cited by Respondent suggests that the term "likely" means that clear and convincing evidence is required in this case. *E.g., Colorado v. New Mexico*, 467 U.S. 310, 315-17 (1984) (applying heightened

standard of proof based on "the unique interests involved in water rights disputes between sovereigns," not because any statute involved required showing that any event was "likely"). Accordingly, Complaint Counsel has the burden of proving each factual issue supporting its claims against Respondent in this case by a preponderance of credible evidence.

B. JURISDICTION

Section 5 of the FTC Act grants the FTC the authority over "unfair or deceptive acts or practices in or affecting commerce" by "persons, partnerships, or corporations . . . ." 15 U.S.C. § 45(a)(1)-(2) (2012).[22] Respondent LabMD, Inc. ("Respondent" or "LabMD") is a privately held Georgia corporation, incorporated in 1996 by Mr. Michael J. Daugherty. F. 24. It is undisputed that Respondent is a corporation. Complaint ¶ 1; Answer ¶ 1. From at least 2001 through approximately January 2014, LabMD was in the business of conducting clinical laboratory tests on urological specimen samples and reporting test results to its physician clients. F. 26. Respondent stipulates that the acts and practices alleged in the Complaint are "in or affecting commerce." F. 30; *see* also F. 28-29.

In its order denying Respondent's November 12, 2013 Motion to Dismiss (*see* Section I.A.2. and footnote 1, *supra*), the Commission held that its jurisdiction over unfair practices extends to a "company's failure to implement reasonable and appropriate data security measures" and that it has jurisdiction over this case. *LabMD*, 2014 FTC LEXIS 2, at *3, *7. Believing the Commission's determination of its jurisdiction to be erroneous, Respondent reserves its jurisdictional challenge for its anticipated appeal to the federal court. RCL 146. Based on the foregoing, the issue of jurisdiction will not be revisited in this Initial Decision. *See In re North Carolina Bd. of Dental Examiners*, 2011 FTC LEXIS 137, at *180-82 (July 14, 2011) (declining to address respondent's state action immunity defense).

[22] Section 4 of the FTC Act defines "corporation," in part, as "any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business for its own profit or that of its members, and has shares of capital or capital stock or certificates of interest . . . ." 15 U.S.C. § 44.

C. LEGAL FRAMEWORK FOR DETERMINING UNFAIR CONDUCT

The Complaint alleges that (1) Respondent failed to provide "reasonable" security for Personal Information[23] on its computer networks, including because Respondent failed to have in place the data security practices specified in the Complaint at ¶¶ 10(a)-(g); and that (2) Respondent's alleged unreasonable data security "caused, or is likely to cause, substantial injury to consumers that is not reasonably avoidable, or offset by benefits to consumers or competition." Complaint ¶¶ 10, 22. Therefore, the Complaint charges, Respondent's alleged unreasonable data security "constitute[s] an unfair practice in violation of Section 5(a) of the FTC Act." Complaint ¶ 23. As authority for finding unfair conduct liability, Complaint Counsel relies on Section 5(n) of the FTC Act, which provides that "[t]he Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

Congress amended the FTC Act in 1994 to add Section 5(n). FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695. The intent of the amendment was not to expand, but to establish an outer limit to the Commission's authority to declare an act or practice unfair. *See* H.R. CONF. REP. 103-617 at 5, FTC Act Amendments of 1994, 1994 WL 385368, at *11-12 (July 21, 1994) (stating that new Section 5(n): "[a]mends section 5 of the Act to *limit* unfair acts or practices to those that: (1) cause or are likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or competition") (emphasis added). The three-part test in Section 5(n) was "intended to codify, as a *statutory limitation* on unfair acts or practices, the principles of the FTC's December 17, 1980, policy statement on unfairness, reaffirmed by a letter from the FTC dated March 5, 1982," in order to provide guidance and to

[23] The parties have stipulated that the term "Personal Information," as used by the parties, means: "Individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. F. 3.

prevent a future FTC from abandoning those principles. S. REP. 103-130, 1993 WL 322671, at *12 (Aug. 24, 1993) (emphasis added); *see* Letter from FTC to Senators Ford and Danforth (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, at *300 (Dec. 21, 1984) ("Policy Statement"); Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (March 5, 1982), reprinted in H.R. REP. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) ("1982 Policy Letter").

According to the Policy Statement, "[u]njustified consumer injury is the primary focus of the FTC Act." Policy Statement, 1984 FTC LEXIS 2, at *307. Moreover, the consumer injury must be substantial, and not "trivial or merely speculative." *Id.* In the 1982 Policy Letter, FTC Chairman Miller reiterated that the Commission's "concerns should be with substantial injuries; its resources should not be used for trivial or speculative harm." 1982 Policy Letter, *supra*. In adopting Section 5(n), Congress noted: "In most cases, substantial injury would involve monetary or economic harm or unwarranted health and safety risks." S. REP. 103-130, 1993 WL 322671, at *13. Furthermore, although a finding of unfair conduct can be based on "likely" future harm, "[u]nfairness cases usually involve actual and completed harms." *Int'l Harvester Co.*, 1984 FTC LEXIS 2, at *248; *accord In re Orkin Exterminating Co.*, 108 F.T.C. 263, 1986 FTC LEXIS 3, at *50 n.73 (Dec. 15, 1986).

Section 5(n) is clear that a finding of actual or likely substantial consumer injury, which is also not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition, is a legal precondition to finding a respondent liable for unfair conduct. *See LabMD*, 2014 FTC LEXIS 2, at *52 (Commission Order on Motion to Dismiss) (holding that determining Respondent's liability in this case requires determining whether the alleged "substantial injury" occurred, and "also whether LabMD's data security procedures were 'unreasonable' in light of the circumstances"); *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 934-35 (N.D. Ill. 2008) ("[S]ubsection (n) . . . requires as a precondition to the FTC's authority to declare an act or practice to be 'unfair' that it be one that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'"). *See also FTC v. Wyndham Worldwide Corp.*, 2015 U.S. App. LEXIS 14839, at **54 (3rd Cir. Aug. 24, 2015) (noting that "[t]he three requirements in § 45(n) may be necessary rather than

sufficient conditions" for finding unfair conduct). As explained below, the preponderance of the evidence in this case fails to show that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury. Accordingly, the Complaint must be dismissed, and it need not, and will not, be further determined whether or not Respondent's data security was, in fact, "unreasonable."[24]

D. CONSUMER HARM ANALYSIS

1. Terminology

As more fully detailed below, Complaint Counsel asserts that the "substantial consumer injury" at issue in this case consists of the monetary losses and other allegedly cognizable injuries that result from identity theft. Complaint Counsel also asserts intangible injuries that allegedly arise as a result of unauthorized disclosure of certain types of Personal Information through a data breach alone, apart from any resulting identity theft. "Identity theft" refers to the use of another person's identity without his or her permission. F. 228. "Identity fraud" refers to the unauthorized use of some portion of another person's information to achieve illicit financial gain. F. 229. Complaint Counsel uses the terms "identity theft" and "identity fraud" interchangeably. Identity theft and identity fraud are distinguishable from a "data breach," in that a data breach refers only to the unauthorized exposure of personal information, while identity theft and identity fraud refer to the improper use of personal information. F. 236.

As a matter of common usage, the generic term "identity theft" may include "identity fraud," new account fraud ("NAF"), existing non-card fraud ("ENCF"), existing card fraud ("ECF"), and medical identity theft. F. 229, 235. NAF is identity fraud perpetrated through the use of another person's personally identifiable information to open new, fraudulent accounts. F. 230. ENCF is identity fraud perpetrated through the use of existing checking or savings accounts or existing loans, insurance, telephone, and utilities accounts. F. 231. ECF is identity fraud perpetrated through the use of existing credit or debit cards and/or their account numbers. F. 232. Medical identity theft, also referred to as medical identity fraud, is the unauthorized use

[24] As detailed in Section II.C.1., *supra*, LabMD wound down its operations beginning in January 2014, and as of May 2014, LabMD's operations were limited to maintaining tissue samples and providing copies of prior test data to its physician clients only via facsimile. F. 36-39. Accordingly, references to LabMD's operations, including with respect to data security, are in the past tense.

of a third party's personally identifiable information to obtain medical products or services, including but not limited to: office visits and consultations, medical operations, and prescriptions. F. 233. Medical identity theft may also involve attempts to fraudulently bill insurance providers. F. 233.

Based on the foregoing, for ease of reference, unless the context indicates otherwise, "identity theft harm" as used in this analysis shall refer to injury arising from the misuse of personal information pursuant to identity theft, medical identity theft, and the other identity theft subtypes referred to above. Also, the terms "harm" and "injury" are used herein interchangeably, and, unless the context indicates otherwise, shall refer to all harms or injuries asserted by Complaint Counsel as meeting the "substantial injury" test set forth in Section 5(n).

2. Overview of Arguments on Substantial Consumer Injury

The Complaint alleges two "security incidents" in connection with Respondent's alleged unreasonable data security (hereafter "Security Incidents"). Complaint ¶¶ 17-21. As to the first Security Incident, the Complaint alleges that a "third party" informed LabMD that a June 2007 insurance aging report generated by LabMD was "available" on a peer-to-peer ("P2P") file-sharing network, through a file-sharing application called LimeWire. Complaint ¶ 17. This insurance aging report, consisting of 1,718 pages, is referred to herein as the "1718 File" and discussed in greater detail in Section III.D.5., *infra*. The second alleged Security Incident avers that, in October 2012, "more than 35 Day Sheets" and "a small number of copied checks" were found in the possession of individuals in Sacramento, California who subsequently pleaded "no contest" to identity theft charges. Complaint ¶ 21. The documents, referred to herein as the "Sacramento Documents," are discussed in greater detail in Section III.D.6, *infra*.

The Order on Post-Trial Briefs, issued on July 16, 2015, specifically directed the parties to address the issue of the substantial consumer injury requirement of Section 5(n) as follows:

> Complaint Counsel shall fully and clearly articulate, and Respondent shall fully and clearly reply to, Complaint Counsel's theory of "substantial injury" in this case, including, without limitation: (1) the specific nature of the substantial injury or injuries asserted; (2) whether such asserted substantial injuries constitute

present or future injuries; and, (3) as applicable, an assessment of the risk and/or likelihood of the asserted substantial injuries.

In re LabMD, Inc., 2015 FTC LEXIS 178, at *8-9 (July 16, 2015).

Having reviewed and considered the totality of Complaint Counsel's post-trial filings, including Complaint Counsel Post-Trial Brief, Proposed Findings of Fact and Conclusions of Law, and replies to Respondent's post-trial filings, Complaint Counsel's argument appears to assert the following as meeting the "substantial injury" requirement in Section 5(n):

- Likely identity theft harm for consumers whose Personal Information was exposed in the 1718 File and the Sacramento Documents, including monetary losses from NAF, ECF, and ENCF, based on an "increased risk" that consumers whose information is exposed in a data breach will suffer identity theft harm;

- Likely medical identity theft harm for consumers whose Personal Information was exposed in the 1718 File,[25] including monetary losses due to fraudulently procured medical products and services, and health and safety risks;

- "Significant risk" of reputational harm, privacy harm, and/or other harms based on stigma or embarrassment, caused by the unauthorized exposure of asserted "sensitive medical information" in the 1718 File; and,

- "Risk" of harm to all consumers whose information is maintained on LabMD's computer network, which Complaint Counsel variously describes as the "risk," "increased risk," or "significant risk," that Respondent's computer network will suffer a future data breach, resulting in identity theft harm, medical identity theft harm, and/or other harm.

See, e.g., CCB 63-72; CCCL 27, 30, 33, 35-40; CCFF §§ 8.2, 8.3, 8.4. *See also* CX0741 (Van Dyke Expert Report); CX0742 (Kam Expert Report).

On the issue of substantial consumer injury, Respondent contends, in summary, that Complaint Counsel has failed to meet its burden of proving actual or likely consumer harm as a result of Respondent's alleged unreasonable data security. Respondent asserts that there is no evidence that any consumer has suffered any actual harm as a result of Respondent's alleged unreasonable data security, and that the evidence fails to show that any harm is probable in the

[25] Complaint Counsel's brief and proposed findings of fact do not address the likelihood of medical identity theft from the exposure of the Sacramento Documents. *See* CCB at 71-72; CCFF § 8.4. To the extent Complaint Counsel asserts that the exposure of the Sacramento Documents is likely to cause medical identity theft harm, as set forth below, the evidence fails to prove that such harm has occurred, or is likely to occur. *See* footnote 38, *infra*.

future. Complaint Counsel replies to this argument that: Section 5(n) does not require proof of actual, completed harms; proof of likely harm is sufficient under Section 5(n); consumers do not necessarily know or investigate when they have suffered identity theft harm; the evidence demonstrates actual harm in the form of reputational and other harms arising from the exposure of the 1718 File; and the evidence demonstrates increased risk and/or significant risk of data breach and resulting injury.

3. Actual or Likely Harm

The record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged failure to employ "reasonable" data security for its computer networks, including in connection with the Security Incidents alleged in the Complaint. Complaint Counsel presented no evidence of any consumer that has suffered NAF, ECF, ENCF, medical identity theft, reputational injury, embarrassment, or any of the other injuries Complaint Counsel describes. Complaint Counsel's response -- that consumers may not discover that they have been victims of identity theft, or even investigate whether they have been so harmed, even if consumers receive written notification of a possible breach, as LabMD provided in connection with the exposure of the Sacramento Documents (F. 212) -- does not explain why Complaint Counsel's investigation would not have identified even one consumer that suffered any harm as a result of Respondent's alleged unreasonable data security.

Complaint Counsel's response to the absence of evidence of actual harm in this case, that it is not legally necessary under Section 5(n) to prove that actual harm has resulted from alleged unfair conduct, because "likely" harm is sufficient, *see, e.g.*, CCRFF 295, 414, 455; CCRB at 131-132; CCCL ¶ 25, fails to acknowledge the difference between the burden of production and the burden of persuasion. The express language of Section 5(n) plainly allows liability for unfair conduct to be based on conduct that has either already caused harm, or which is "likely" to do so. *See Wyndham*, 2015 U.S. App. LEXIS 14839, at **21. However, as shown *infra*, the absence of any evidence that any consumer has suffered harm as a result of Respondent's alleged unreasonable data security, even after the passage of many years, undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless "likely" to occur. This is

particularly true here, where the claim is predicated on expert opinion that essentially only theorizes how consumer harm could occur. Given that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.

In light of the inherently speculative nature of predicting "likely" harm, it is unsurprising that, historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm. Indeed, the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted "likely" harm alone. For example, in *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988), the appellate court upheld the Commission's finding of substantial injury, based on undisputed evidence that Orkin's failure to honor consumers' contracts generated, during a four-year period, more than $7 million in revenues from renewal fees paid by consumers to which Orkin was not entitled. In *FTC v. Accusearch, Inc.*, 2007 U.S. Dist. LEXIS 74905 (Sept. 28, 2007), *aff'd*, 570 F.3d 1187 (10th Cir. 2009), on the issue of substantial injury, the court stated: "The range of injuries experienced by the consumers whose phone records were sold fits squarely within the categories of harm contemplated by the FTC's policy," including "documented economic harm" in the form of "actual costs associated with changing telephone carriers and addressing necessary upgrades to the security of the accounts." *Id.* at *23-24.

The substantial consumer injury supporting unfair conduct liability in *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1154 (9th Cir. 2010), was the issuance of fraudulent checks totaling over $4 million, caused by the defendant's faulty "Qchex" system. And, in *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012), the defendant's website marketing of its online auction product caused thousands of consumers to incur unauthorized monthly charges ranging from $29.95 to $59.95, with an approximate total of $18.2 million in consumer losses. *See also FTC v. Windward Mktg., Ltd.*, 1997 U.S. Dist. LEXIS 17114 at *2, *31-32 (N.D. Ga. Sept. 30, 1997) (unauthorized demand drafts paid against consumers' bank accounts as a result of fraudulent telemarketing scheme); *Int'l Harvester*, 1984 FTC LEXIS 2, at *255 (death and serious injury resulting from failure to disclose known defects in respondent's tractors). Finally, in *Wyndham*, 2015 U.S. App. LEXIS 14839, which is the only court case that has upheld the

FTC's authority to bring an unfair conduct claim based upon alleged unreasonable data security, the court, in denying the defendant's motion to dismiss, noted, *inter alia*, that "[o]n three occasions in 2008 and 2009 hackers successfully accessed Wyndham['s] computer systems . . . [and] stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges." *Id.* at **3.

Section 5(n) does not define the meaning of "likely" injury. Where a statute does not define a term, it is construed in accordance with its ordinary meaning. *FDIC v. Meyer*, 510 U.S. 471, 476 (1994) (using Black's Law Dictionary to define the meaning of statutory term, "cognizable"). The Merriam-Webster dictionary states that "likely" is "used to indicate the chance that something will happen," and is primarily defined as "having a high probability of occurring or being true." *Merriam-Webster.com.*, *at* http://www.merriam-webster.com/dictionary/likely). In *Southwest Sunsites v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1986), the court interpreted the Commission's deception standard, which required proof that a practice is "likely to mislead" consumers, to require proof that such deception was "probable, not possible . . . ." Based on the foregoing, "likely" does not mean that something is merely possible. Instead, "likely" means that it is probable that something will occur.

Complaint Counsel argues that the requirement of proving that injury is "likely" can be met by evidence of a "significant risk" of injury, citing a footnote in the Policy Statement in which the Commission stated: "An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, *or if it raises a significant risk of concrete harm*." 1984 FTC LEXIS 2, at *307 n.12 (emphasis added); *see also LabMD*, 2014 FTC LEXIS 2, at *54. However, although Congress refers to the Policy Statement in explaining the meaning of Section 5(n), the Senate Report states in part: "Consumer injury may be 'substantial' under this section if a relatively small harm is inflicted on a large number of consumers *or if a greater harm is inflicted on a relatively small number of consumers*." S. REP. 103-130, 1993 WL 322671, at *13 (emphasis added). The omission of the Commission's "significant risk" language in explaining "substantial injury" indicates that Congress considered but rejected this standard. Congress instead enacted the requirement that, to be declared "unfair," there must be proof that actual harm has occurred, or in the absence of proof of actual, completed harm, proof that the

challenged conduct is "likely" to cause harm in the future. Moreover, although some courts have cited the "significant risk" language from the Policy Statement, *see, e.g.*, *Neovi*, 604 F.3d at 1157, the parties have not cited, and research does not reveal, any case in which unfair conduct liability has been imposed without proof of actual, completed harm, based instead upon a finding of "significant risk" of harm.[26]

Based on the foregoing, to the extent "significant risk," or "increased risk," of injury implies a lower standard of proof than "likely" injury, such a standard would conflict with the express language of Section 5(n). It is unnecessary to resolve any apparent conflict, however, because, as more fully explained below, even under Complaint Counsel's asserted "significant risk" standard for proving likely harm, Complaint Counsel has failed to prove that Respondent's alleged unreasonable data security is "likely" to cause substantial consumer injury.

Section 5(n) is a three-part test, and all three parts must be proven before an act or practice can be declared "unfair." 15 U.S.C. § 45(n). *See Orkin Exterminating Co.*, 849 F.2d at 1364 ("[T]o justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.") (*quoting* Policy Statement at 36); *see also Windward Mktg.*, 1997 U.S. Dist. LEXIS 17114, at *30. Accordingly, Complaint Counsel's failure to meet its burden of proving the first prong of the three part test – that Respondent's conduct caused, or is likely to cause, substantial consumer injury – is fatal to its case, and any factual determinations regarding the additional two prongs of the unfair conduct test – that substantial consumer injury is not

[26] In *American Financial Services v. FTC*, 767 F.2d 957 (D.C. Cir. 1985), the Court of Appeals for the District of Columbia Circuit upheld a credit practices rule that prohibited wage assignments and household good security interests, finding substantial evidence that these practices were unfair. Regarding the evidence of substantial injury in the rulemaking record, the court stated: "The harms to consumers resulting from the use of HHG security interests and wage assignments identified by the Commission on the basis of the rulemaking record are neither trivial or speculative nor based merely on notions of subjective distress or offenses to taste [and therefore they] result in *or* create a significant risk of substantial economic and monetary harm to the consumer as well as potential deprivations of their legal rights." 767 F.2d at 975 (emphasis added). *American Financial Services* is not precedent that liability can be based on a "significant risk of harm" alone, since the rulemaking record in that case contained substantial evidence that the prohibited provisions had indeed caused financial and other harm to consumers. 767 F.2d at 973-75. It should also be noted that *American Financial Services* involved review of a rulemaking, not an adjudication of individual liability, and was decided before the 1994 enactment of Section 5(n). As noted above, the legislative history of Section 5(n) indicates that Congress rejected "significant risk" as a basis for finding substantial consumer injury.

reasonably avoidable by consumers, and is not outweighed by benefits to consumers or competition – would be superfluous and, accordingly, need not, and will not, be made.

4. Complaint Counsel's Proffered Consumer Injury Experts

As noted above, Complaint Counsel's contention that Respondent's alleged unreasonable data security is likely to cause harm is predicated upon expert opinion from two proffered experts, Mr. Rick Kam and Mr. James Van Dyke.

Mr. Kam is president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration, and is a Certified Information Privacy Professional. F. 9. According to Mr. Kam, his expertise includes "identifying and remediating the consequences of identity theft and medical identity theft" and "helping organizations develop policies and solutions" to safeguard sensitive personal information. F. 10. Mr. Kam was asked "to assess the risk of injury to consumers caused by the unauthorized disclosure" of their personal information. F. 11. For the purposes of this analysis, Mr. Kam assumed that LabMD failed to provide reasonable security for consumer information on its computer networks. F. 244. In summary, Mr. Kam opined that LabMD's alleged unreasonable data security "is likely to cause substantial injury to consumers and puts them at significant risk of identity crimes." CX0742 (Kam Expert Report at 9). Mr. Kam's more detailed opinions are addressed *infra* in the context of the particular harms alleged in this case.

Mr. Van Dyke is the founder and president of Javelin Strategy & Research ("Javelin"), a research company whose activities include publishing results from an annual identity fraud survey and an associated report. F. 12. According to Mr. Van Dyke, he is experienced in how sensitive information is used and has expertise in identity theft. F. 14. Mr. Van Dyke was asked to "assess the risk of injury to consumers" whose personally identifiable information "has been disclosed by [LabMD] without authorization." F. 15. He was also asked to assess the risk of injury to those consumers whose information "was not adequately protected from unauthorized disclosure." F. 15. Mr. Van Dyke assumed, as did Mr. Kam, that LabMD failed to provide reasonable security for personal information maintained on its computer networks. F. 257. In general, Mr. Van Dyke opined that consumers whose information was disclosed in the 1718 File and the Sacramento Documents are significantly more likely to become victims of identity theft

and its various subtypes. CX0741 (Van Dyke Expert Report at 3, 6). Mr. Van Dyke also prepared what he called "projections" of the number of such identity theft victims in this case and the financial losses that will result, were identity theft to occur. *Id*. at 6-14. Mr. Van Dyke further opined that LabMD's alleged unreasonable data security "risked exposing" all consumers whose personal information is maintained by LabMD to "a likelihood" of identity theft harm, even if such personal information has not yet been disclosed. *Id.* at 13. The specifics of Mr. Van Dyke's opinions are addressed in relation to the specific harms asserted by Complaint Counsel, *infra*.

5. The 1718 File Incident

a. Summary of facts

The "1718 File" is a LabMD insurance aging report, containing 1,718 pages, dated June 2007, with the filename "insuranceaging_6.05.071.pdf" and is the document identified as the "[peer-to-peer] insurance aging file" in Paragraphs 17, 18, 19, and 21 of the Complaint. F. 1, 73, 78. On or about February 25, 2008, Mr. Richard Wallace, a forensic analyst then employed by a breach detection and remediation services company known as Tiversa Holding Company ("Tiversa"), was performing searches on a peer-to-peer network when he discovered and downloaded the 1718 File. F. 100, 102-104, 121. The 1718 File was downloaded from an IP address in Atlanta, Georgia, which belonged to LabMD. F. 121. These events, further addressed below, are referred to herein as the "1718 File Incident." F. 78.

By way of background, peer-to-peer file-sharing applications enable one computer user to make a request to search for all files that have been made available for sharing by another (or "host") computer that is also using the same file-sharing application. F. 63. A file that is being "shared" or "made available for sharing," on a peer-to-peer network is available to be downloaded by another computer user on the same peer-to-peer network. F. 66. Typically, users will search using terms related to the particular file they hope to find and receive a list of files that are possible matches. F. 65. The user then chooses a file he or she wants to download from the list, which is then downloaded from the peers who possess that file. F. 65. The contents of a file are not exposed until the file is downloaded. F. 68.

Peer-to-peer networks are often used to share music, videos, pictures, and other materials. F. 64. In 2008, LimeWire was a peer-to-peer file-sharing application, and one of a number of applications that used a protocol called Gnutella. F. 69. Gnutella is a program that connects computers together in a direct peer-to-peer fashion to facilitate file sharing through searching and downloading. F. 70.

In May 2008, Tiversa contacted LabMD and told LabMD that the 1718 File was available through LimeWire. F. 88. LabMD investigated and determined that LimeWire was installed on a computer belonging to LabMD's billing manager (the "Billing Computer") and that the 1718 File was among the files made available for sharing. F. 89-91. After searching all of LabMD's computers, it was determined that no other LabMD computers had file-sharing applications installed. F. 90, 93-94. LabMD removed LimeWire from the Billing Computer in May 2008. F. 92. In addition, Mr. John Boyle, LabMD's vice president of operations and general manager from November 1, 2006 until the end of August 2013, assigned LabMD Information Technology ("IT") Specialist Allison Simmons, and later, IT Manager Jeffrey Martin, to search peer-to-peer networks to look for the 1718 File. F. 95. Specifically, in May 2008, Ms. Simmons searched peer-to-peer networks from her home computer to look for the 1718 File. F. 96. She searched multiple times for at least a month thereafter for the file name insuranceaging_6.05.071.pdf, partial file names, and anything with the name LabMD associated with it. F. 96. In 2013, Mr. Martin searched peer-to-peer networks for the 1718 File multiple times over the course of a few months, using the file name, as well as the terms "LabMD," "patient," and "aging." F. 97. The searches performed by Ms. Simmons and Mr. Martin did not locate the 1718 File on any peer-to-peer network. F. 98.

In addition, in 2009, Mr. Wallace, of Tiversa, searched Tiversa's internal database of peer-to-peer sharing downloads (Tiversa's "Data Store") to determine if Tiversa's automatic searching system, which uses a series of algorithms to search all peer-to-peer networks, had downloaded the 1718 File. F. 100, 147. Mr. Wallace determined that the 1718 File had not been downloaded to the Data Store. F. 147. To Mr. Wallace's knowledge, the 1718 File never spread beyond the original disclosing source, LabMD. F. 154.

In 2008, Tiversa was a "research partner" of Professor Eric Johnson, then of Dartmouth College, in connection with an article that Professor Johnson was writing. F. 169, 170. Tiversa's role in the research was to conduct searches for Professor Johnson and to forward files to him for further analysis. F. 172. All the files examined in Professor Johnson's research for his article were provided to him by Tiversa. F. 172. Professor Johnson referred to the 1718 File in his article, published in February 2009, titled "Data Hemorrhages in the Health-Care Sector." F. 169, 171. Tiversa had provided the 1718 File to Professor Johnson. F. 178. However, the evidence fails to prove that the 1718 File was discovered as a product of Professor Johnson's search protocol, notwithstanding any contrary representation in his article. F. 173-175, 178-179. Professor Johnson did not share the sensitive information in the 1718 File with anyone. F. 181.

In 2009, Tiversa, who had been communicating with the FTC regarding peer-to-peer file-sharing matters (F. 133-134), identified LabMD to the FTC as one of the entities that Tiversa discovered had shared personal information of consumers on peer-to-peer networks. F. 139-142. Tiversa also provided the 1718 File to the FTC.[27] F. 138.

b. Overview of analysis

Complaint Counsel argues that the exposure of the 1718 File on the Gnutella network constitutes evidence that Respondent's data security practices are likely to cause substantial harm, and that consumers whose Personal Information was exposed in the 1718 File are at "significantly higher risk than the general public of becoming a victim of identity theft and medical identity theft, or of experiencing other privacy harms[. Therefore,] the failure to secure the 1718 File is likely to cause them substantial injury." CCB 69. Respondent argues that other than Tiversa, Professor Johnson, and the FTC, no one outside of LabMD downloaded or viewed

[27] Tiversa did not want the FTC to issue a formal information request, such as a Civil Investigative Demand ("CID"), directly to Tiversa because Tiversa had been in talks regarding a possible acquisition and Tiversa's chief executive officer, Mr. Boback, did not want Tiversa to be "in the middle of a civil investigative demand." F. 135. Instead, Mr. Boback wanted the CID to be issued to a third party to "separate" the CID from Tiversa, "to try to create some distance" from Tiversa. F. 135. Accordingly, Tiversa created an entity called "The Privacy Institute," so Tiversa could avoid providing information to the FTC under Tiversa's name. F. 136. The Privacy Institute was created only for the purpose of receiving the CID from the FTC. F. 136. Upon Tiversa's request, the FTC issued the CID for Tiversa's information and documents to the Privacy Institute. F. 137-138. Whether or not this entire process met the requirements of all applicable law, rules, and regulations has not been determined in the instant case.

the contents of the 1718 File. Respondent further argues that there is no evidence that any consumer has suffered any harm from the exposure of the 1718 File.

The evidence shows that the 1718 File was available for peer-to-peer sharing through LabMD no earlier than June 2007 (the date of the document) until May 2008, when Respondent removed LimeWire from the Billing Computer. F. 78, 92, 99. Although the 1718 File was available for downloading during this period, the evidence fails to show that the 1718 File was in fact downloaded by anyone other than Tiversa, who obtained the document in February 2008. Tiversa provided the 1718 File to Professor Johnson and to the FTC. F. 138, 142, 178. Evidence in the record provided by Tiversa and its chief executive officer and corporate designee Mr. Robert Boback, claiming that Tiversa found the 1718 File in "multiple locations" on peer-to-peer networks, including at IP addresses belonging to suspected or known identity thieves, is given no weight. As summarized in Section I.B.2., and detailed in Section II.D.3. and 4., *supra*, such evidence, including without limitation, Mr. Boback's 2013 discovery deposition, Mr. Boback's 2014 trial deposition testimony, and a Tiversa-provided exhibit, CX0019, is unreliable, not credible, and outweighed by credible contrary testimony from Mr. Wallace. Furthermore, Complaint Counsel no longer argues, as it did in its pre-trial brief, that the 1718 File was in fact downloaded by anyone other than Tiversa. In summary, Complaint Counsel has failed to prove that the 1718 File was acquired, viewed, or otherwise disclosed to anyone other than Tiversa, Professor Johnson, and the FTC. Any other assertion or conclusion regarding the extent of the exposure of the 1718 File is pure, unsupported speculation.

As further discussed below, the evidence fails to demonstrate that the exposure of the 1718 File placed the consumers whose Personal Information was exposed in the 1718 File "at significantly higher risk" of harm, or that such exposure caused, or is likely to cause, identity theft harm, medical identity theft harm, or reputational or "other" harm, as argued by Complaint Counsel.

c. Identity theft harm

i. Mr. Rick Kam

Complaint Counsel's arguments, that consumers whose information was contained in the

1718 File are at "significantly higher risk" of becoming victims of identity theft, and are "likely" to suffer identity theft harm, rely on the opinion of its proffered expert, Mr. Kam. *See* CCB at 69, *citing* CCFF 1667, 1668. Mr. Kam evaluated the risk of identity theft harm resulting from an unauthorized disclosure of personal information on the basis of four risk factors, including: (1) the nature of the information exposed; (2) "to whom the disclosure was made [in order] to determine whether the person possessing the information presents a low risk of misuse, or a higher risk of misuse, such as an identity thief"; (3) whether the information was "actually acquired or viewed"; and (4) whether "the data is still available for others to misuse." F. 238-239. Mr. Kam then applied the foregoing risk factors to conclude that the exposure of the 1718 File poses a significant risk of identity theft harm. CX0742 (Kam Expert Report at 18-19).

Although Complaint Counsel announced it would not rely on expert opinion based on the testimony of Mr. Boback or on CX0019, *see* Section I.B.2., *supra*, Mr. Kam's opinion, upon which Complaint Counsel does rely, is expressly based on evidence provided by Mr. Boback that Tiversa had found the 1718 File at various IP addresses between 2008 and 2011; that one of the IP addresses belonged to a suspected identity thief; and that Tiversa found the 1718 File to be still available on peer-to-peer networks in 2013. F. 240-241.[28] As discussed above, this evidence is unreliable, not credible, and outweighed by credible contrary testimony from Mr. Wallace. For this reason, Mr. Kam's opinions that the exposure of the 1718 File is likely to cause, or presents a "significant risk" of, identity theft harm is entitled to, and is given, no weight.

Indeed, applying Mr. Kam's four risk factors, above, to the facts of this case, it is at least as likely, if not more likely, that the exposure of the 1718 File presents a low risk of identity theft harm. In the instant case, the evidence fails to show that the 1718 File was disclosed to and viewed by anyone other than Tiversa, Professor Johnson, and the FTC, and there is no contention, or evidence, that the foregoing persons or entities present a threat of harming consumers. This is in stark contrast to cases relied upon by Complaint Counsel where Personal Information was allegedly obtained by computer hackers and used to commit credit card fraud.

[28] *See also* Kam, Tr. 519 (explaining that he relied upon a report published by the SANS Institute, the SANS Health Care Cyberthreat Report, published in 2014, based upon Mr. Boback's discredited testimony about the discovery of the 1718 File on a peer-to-peer network in 2013).

See Wyndham, 2015 U.S. App. LEXIS 14839, at **3 (court stating that hackers accessed Wyndham's computer systems on three occasions and stole personal and financial information leading to over $10.6 million dollars in fraudulent charges); *Remijas v. Neiman Marcus Group, LLC*, 2015 U.S. App. LEXIS 12487 at **2-3, **8-13 (7th Cir. July 20, 2015) (court stating that hackers accessed Neiman Marcus' computer systems and stole financial information leading to fraudulent use of 9,200 consumers' credit cards).

Significantly, the court in *Neiman Marcus*, in concluding that the plaintiffs had demonstrated sufficient injury to obtain Article III standing, remarked: "[I]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at **12. Here, in contrast, the evidence fails to show any computer hack for purpose of committing identity fraud. Rather, the evidence shows that the 1718 File was obtained by Tiversa from a peer-to-peer network, F. 121-122, and that Tiversa's purpose in obtaining this and other files available from peer-to-peer networks was to then induce companies with an interest in protecting such information to purchase Tiversa's monitoring or remediation services. F. 100, 108-118. Unlike in *Neiman Marcus*, it cannot be presumed that the purpose of Tiversa's act of downloading the 1718 File from a peer-to-peer network was to make fraudulent credit card charges, assume identities, or otherwise harm the consumers whose information is contained in the 1718 File.

In addition, the evidence shows that the 1718 File was no longer available for sharing by LabMD as of May 2008 (F. 99), and the evidence fails to show that the 1718 File remained available on peer-to-peer networks after May 2008. *See* F. 95-98, 153-154. For this reason as well, the evidence fails to prove that the exposure of the 1718 File presents a significant risk of identity theft harm or is likely to cause identity theft harm.

ii. Mr. James Van Dyke

Complaint Counsel's assertion that consumers whose Personal Information was exposed in the 1718 File are at significantly higher risk than the general public of suffering identity theft harm is also based upon the opinions of Mr. Van Dyke, which Mr. Van Dyke derived from the

Javelin 2013 Identity Fraud Survey ("2013 Javelin Survey") and the Javelin 2014 Identity Fraud Report ("2014 Javelin Report"). CCB at 69, citing CCFF 1506-1512; F. 252. As noted above, Mr. Van Dyke, is the founder and president of Javelin. F. 12.

Specifically, Complaint Counsel relies on a statistic reported in the 2013 Javelin Survey that 30.5% of survey respondents who reported being notified within the 12 months preceding the survey that their "personal or financial information ha[d] been lost, stolen, or compromised in a data breach (*i.e.*, data breach victims)," also reported experiencing identity theft within the 12 months preceding the survey ("identity theft rate"). CX0741 (Van Dyke Expert Report at 6-8 and Attachment 1). The 2013 Javelin Survey further stated that 2.7% of those survey respondents who reported they had *not* been notified during the 12 months preceding the survey that they were data breach victims also reported suffering identity theft harm during that same 12-month period. CX0741 (Van Dyke Expert Report at 6-8). Accordingly, Complaint Counsel argues, consumers whose information was exposed in the 1718 File are at a "significantly higher risk" or have an "increased risk" of becoming identity theft victims, and are therefore likely to suffer identity theft harm.[29]

Complaint Counsel also relies on Mr. Van Dyke's projections of the number of 1718 File consumers that will become identity theft victims, and the monetary losses that these consumers will incur as a result. According to Mr. Van Dyke, based on the 2013 Javelin Survey: (1) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their Social Security number ("SSN") was disclosed in a data breach also reported experiencing new account fraud within the preceding 12 months, at an average consumer loss of $449; (2) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing existing non-card fraud within the preceding 12 months, at an average consumer loss of $207; and (3) 13.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing

[29] Mr. Van Dyke also opined that "[t]he circumstances of the unauthorized exposure of the" 1718 File "only stand to make identity fraud more likely" than the 30% identity theft rate found in the 2013 Javelin Survey, based on Mr. Boback's discredited testimony that the 1718 File "was found at four IP addresses, on each of which Tiversa found unrelated consumer identity information." CX0741 (Van Dyke Expert Report at 8). Complaint Counsel does not rely on this particular opinion in its brief or proposed findings of fact.

existing card fraud within the preceding 12 months, at an average consumer loss of $106. CX0741 (Van Dyke Expert Report at 8-12). Mr. Van Dyke applied these percentages and figures to the number of consumers listed in the 1718 File to calculate the number of expected identity theft victims and the expected financial impact. *Id*. However, Mr. Van Dyke did not conduct a survey of the consumers listed on the 1718 File. F. 255.

For several reasons, the 2013 Javelin Survey, the 2014 Javelin Report, and Mr. Van Dyke's opinions based thereon, are not persuasive in proving that those consumers whose Personal Information was exposed in the 1718 File are likely to suffer identity theft harm. First, and perhaps most important, Complaint Counsel's suggested inference, based on the 2013 Javelin Survey, that 30% of the consumers whose data was contained in the 1718 File have suffered, or will suffer, identity theft harm, is unpersuasive, in light of the absence of any evidence that any such consumer, in fact, has been so harmed, despite the passage of more than seven years since exposure of the 1718 File. If it were true that 30% of the consumers affected by the 1718 File exposure are likely to suffer identity theft harm, logically, it would be expected that the government, in the many years of investigation and litigation of this matter, would have discovered and identified at least one such consumer who has experienced identity theft harm. The same logic renders unpersuasive Mr. Van Dyke's predictions of the number of consumers that will suffer NAF, ECF, or ENCF and resulting monetary losses.

As noted above, Complaint Counsel's assertion, based on expert opinion, that it may take "months or years" for a consumer to discover they have been victimized by identity theft (*see* CCFF 1578-1580), does not explain why the government, over the past seven years, in the course of investigating and litigating this case, would not have located and identified any such victims. *See* Section III.D.2., 3. In summary, in the instant case, the absence of evidence that identity theft harm has occurred in the seven years since the exposure of the 1718 File undermines the persuasive value of expert opinion that such harm is, nonetheless, "likely" to occur. *See In re McWane, Inc.*, 2013 FTC LEXIS 76, at *730-31 (May 8, 2013) (finding that the absence of evidence that prices rose after alleged agreement to raise prices undermined assertion that such agreement existed). Fairness dictates that reality must trump speculation based on mere opinion.

Second, results from the 2013 Javelin Survey are not probative as a temporal matter. As discussed above, the 1718 File was made available for sharing no earlier than June 2007; LabMD discontinued its sharing of the document in May 2008; and the evidence fails to show that the 1718 File was available on peer-to-peer networks after May 2008. The 2013 Javelin Survey measured the effect of data breaches occurring five years later, in 2013, and Complaint Counsel points to no evidence from which it could be concluded that the incidence of identity theft for exposures in 2013 is predictive of identity theft harm for an exposure five years earlier, in 2008. Indeed, rather than select and use data from 2008, the most relevant point in time, Mr. Van Dyke selected the 2013 Javelin Survey and 2014 Javelin Report for the bases of his calculations specifically because, in 2013, Mr. Boback testified that Tiversa had located the 1718 File on peer-to-peer networks in four locations, which testimony has been thoroughly discredited. F. 253. Moreover, according to the yearly Javelin Identity Fraud surveys for 2010 through 2013, as set forth in Mr. Van Dyke's report, the identity fraud rate for data breach victims in 2013 was significantly higher than the identity fraud rate for data breach victims in 2010, a point closer in time to the exposure of the 1718 File. CX0741 (Van Dyke Expert Report at 8, Figure 1 (depicting 11.8% rate in 2010, 18.9% rate in 2011, 22.5% in 2012, and 30.5% in 2013)).

Third, it is not apparent that the data breach victims surveyed by the 2013 Javelin Survey are similarly situated to the consumers whose Personal Information was exposed in the 1718 File, such that any identity theft rate derived from the 2013 Javelin Survey can be extrapolated to predict identity theft harm for the 1718 File consumers. As noted above, the limited time duration that the 1718 File was available for downloading, and the limited extent of actual exposure of the 1718 File, including the fact that the 1718 File was downloaded by Tiversa for business purposes, and not for identity theft purposes, are factors that militate against the risk of identity theft harm in this case. The evidence fails to show the types of data breaches reported in the 2013 Javelin Survey are comparable to the type of data exposure that occurred in the 1718 File Incident.

For all the foregoing reasons, the evidence fails to show that the exposure of the 1718 File has caused, or is likely to cause, identity theft harm.

d. Medical identity theft harm

Relying on expert opinion, Complaint Counsel asserts that the exposure of the 1718 File is likely to result in medical identity theft harm. *See* CCB at 70-71. Specifically, Mr. Van Dyke opined that "medical identity fraud remains a threat to consumers," citing survey responses as to the frequency of medical identity theft. He further opined that health insurance policy information and SSNs, which are found in the 1718 File, "can be utilized" by criminals to commit medical identity frauds, such as procuring procedures, services, and products. CX0741 (Van Dyke Expert Report at 13-14). Mr. Van Dyke also opined that such frauds, when they occur, "can burden affected consumers with financial costs related to unpaid medical bills from unauthorized procedures, products, or services, as well as direct physical harm in those cases where a change is made to a consumer's medical records that could result in improper or unnecessary treatments." *Id.* The foregoing is not an opinion that medical identity theft is likely to result from the exposure of the 1718 File, but is little more than a statement of Mr. Van Dyke's belief that identity theft criminals "could" use information in the 1718 File, if they obtained it, and his opinion of the financial and other harms that "could" result, if medical identity theft were to occur. However, the evidence fails to show that any identity theft criminals have obtained the 1718 File, and therefore the projection of resulting harms from medical identity theft is pure theory and speculation.

Complaint Counsel also relies on predictions by Mr. Kam that the 1718 File consumers are subject to "health and safety" risks resulting from medical identity theft, such as misdiagnosis or mistreatment of illness. CX0742 (Kam Expert Report at 20). Mr. Kam explained that if an identity thief's health information "merges" with that of the identity theft victim, inaccuracies in medical records could result and cause mistreatment or misdiagnoses. Kam, Tr. 426-430. Mr. Kam further predicted, derived from an "estimated base rate" for medical identity theft of 0.0082, that at least 76 of the 9,300 consumers identified in the 1718 File will become victims of medical identity theft, and that 36% of these individuals will each suffer out-of-pocket costs for fraudulently procured medical services among other expenses in the amount of $18,660. CX0742 (Kam Expert Report at 19-20).[30] Mr. Kam based these

[30] Mr. Kam opined that these losses from medical identity theft include payments required as a result of a "lapse" of health insurance. (Kam, Tr. 422). However, Mr. Kam failed to explain this assertion.

opinions on statistics as to the frequency and impact of medical identity theft reported by the 2013 Survey on Medical Identity Theft by the Ponemon Institute ("2013 Ponemon Survey"). F. 246. Mr. Kam's opinions are unpersuasive to demonstrate that the exposure of the 1718 File is likely to cause medical identity theft harm, as explained below.

As stated previously, there is no evidence that any consumer has suffered any of Mr. Kam's predicted harms as a result of the exposure of the 1718 File, notwithstanding the passage of more than seven years since the exposure of the 1718 File in 2008.[31] Furthermore, the 2013 Ponemon Survey lacks significant probative value, given that it measured the rate and impact of medical identity theft for 2013, five years after the 2008 disclosure of the 1718 File. *See* F. 246. Moreover, numerous facts detract from the reliability of the 2013 Ponemon Survey. The response rate to the 2013 Ponemon Survey was only 1.8%, which Mr. Kam agreed creates a non-response bias, *i.e.*, a failure to take into account that those who were surveyed, but did not respond, might have a different answer to the question. F. 247. In addition, the 2013 Ponemon Survey had a sampling frame bias[32] and compensated respondents for completing the survey within a set time period. F. 248-249. Also significant is that, to the extent the 2013 Ponemon Survey is reliable, the accompanying report notes that medical identity theft rarely occurs from data breaches or the acts of an identity thief. F. 250. Rather, the 2013 Ponemon Survey reports that medical identity theft is far more likely to result from a consumer's knowingly sharing personal identification or medical credentials or the unauthorized use of such information by a family member. F. 250. Mr. Kam agreed that medical identity theft rarely occurs from data breaches or the acts of an identity thief and acknowledged that most occurrences of medical identity theft result from someone knowingly sharing their personal information or medical credentials and from instances where one family member took another family member's personal information or medical credentials without consent. F. 251.

[31] Although Mr. Kam did not expressly rely on the discredited and unreliable testimony from Mr. Boback as to the "spread" of the 1718 File for his opinions on the likelihood of medical identity theft, this evidence was clearly considered by Mr. Kam (CX0742 (Kam Expert Report at 6)) and it cannot be assumed that Mr. Kam's opinions were not influenced by his review of Mr. Boback's testimony.

[32] The 2013 Ponemon Survey's sampling frame contained individuals who were prescreened from a larger sample on the basis of their identity theft or identity fraud experience. The 2013 Ponemon Survey acknowledged, and Mr. Kam agreed, that this resulted in a sampling frame bias. F. 248.

For all the foregoing reasons, the evidence fails to support the conclusion that medical identity theft harm is likely to result from the exposure of the 1718 File that occurred in this case.

e. Reputational and other harms

Finally, relying on expert opinion from Mr. Kam, Complaint Counsel argues that the exposure of the 1718 File alone, without any resulting identity theft, is likely to cause "reputational and other harms" to those consumers. Specifically, Complaint Counsel asserts that the 1718 File disclosed some current procedural terminology ("CPT") codes that indicate testing for "sensitive conditions," such as sexually transmitted diseases, including HIV, prostate cancer and testosterone levels, and that disclosure of such testing causes harm in the form of stigma or embarrassment. *See* CCB at 71.

Mr. Kam opined that there is a "significant risk" of reputational harm for those consumers whose CPT codes indicate tests for prostate cancer, herpes, hepatitis, HIV, and testosterone levels. Kam, Tr. 447-448; CX0742 (Kam Expert Report at 9). Further, he opined that disclosure of the mere fact that such a test was performed, even without disclosure of any associated condition or diagnosis, "could cause" consumers to feel embarrassed, upset, or stigmatized. Kam, Tr. 448; CX0742 (Kam Expert Report at 16, 21).[33] However, as Mr. Kam acknowledged, disclosure of a CPT code, by itself, does not disclose what test was performed. F. 83. In fact, Mr. Kam testified that he had to rely on a Google search to determine what the CPT codes stood for. F. 83. Moreover, given the subjective nature of feelings of stigma, upset, or embarrassment, and the fact that Complaint Counsel did not identify a single person affected by the 1718 File disclosure who experienced these feelings as a result of the 1718 File disclosure, expert opinion that these feelings "can" occur carries little or no weight. *Compare Accusearch,* 2007 U.S. Dist. LEXIS 74905, at *23-24 (noting undisputed fact that some consumers whose phone records were sold to stalkers and abusers had suffered actual and severe emotional harm).

[33] Mr. Kam also opined that exposure of CPT codes could lead to negative changes to life, health, and disability insurance. CX0742 (Kam Expert Report at 21). However, Mr. Kam failed to persuasively explain how disclosure of the mere fact that testing was performed, without further information, could result in negative changes to insurance.

In addition, subjective feelings such as embarrassment, upset, or stigma, standing alone, do not constitute "substantial injury" within the meaning of Section 5(n). According to the legislative history of Section 5(n), "[e]motional impact and more subjective types of harm alone are not intended to make an injury unfair." S. REP. 103-130, 1993 WL 322671, at *13; *see also* 1982 Policy Letter, *reprinted in* H.R. Rep. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) ("As a general proposition, substantial injury involves economic or monetary harm and does not cover subjective examples of harm such as emotional distress . . ."). While the Commission has stated that "[i]n an extreme case, . . . where tangible injury could be clearly demonstrated, emotional effects might possibly be considered as the basis for a finding of unfairness," Policy Statement, 1984 FTC LEXIS 2, at *308 n.16, in the instant case, there is no demonstrated tangible injury to consumers from the exposure of the 1718 File. *Compare Accusearch*, 2007 U.S. Dist. LEXIS 74905, at *22-24 (finding conduct caused economic harm and health and safety risks in addition to emotional harm).

Accordingly, the evidence fails to prove that consumers are likely to suffer the asserted "reputational and other harms" as a result of the exposure of the 1718 File. Even if the evidence demonstrated such harms, because the evidence fails to show any tangible injury from the exposure of the 1718 File, the subjective "reputational and other harms" alleged by Complaint Counsel do not constitute sufficient "substantial injury" under Section 5(n).

f. Conclusion

For all the foregoing reasons, the evidence fails to prove that consumers whose information was contained in the 1718 File have suffered, or are likely to suffer, substantial injury as a result of the exposure of the 1718 File. Therefore, the exposure of the 1718 File does not support Complaint Counsel's assertion that Respondent's data security practices are likely to cause substantial consumer harm.[34]

[34] Complaint Counsel also argues that consumer harm is likely from the 1718 File Incident because the 1718 File was made available for sharing on the Gnutella network where any Gnutella user "could" access it. CCB at 69. Evidence that anyone "could" have accessed the 1718 File during the limited period that the 1718 File was made available for sharing carries little probative weight, especially since the evidence fails to show that anyone other than Tiversa, Professor Johnson, and the FTC actually viewed the 1718 File; or that any consumer listed in the 1718 File, in the seven years since the exposure of the 1718 File, has actually suffered any harm as a result of the availability of the 1718 File.

6. The Sacramento Incident

a. Summary of facts

On October 5, 2012, officers of the Sacramento California Police Department (the "SPD") conducted a search of a house in Sacramento, California in connection with an investigation into possible utility bill fraud. F. 189-192. In that house, the SPD discovered what was believed to be evidence of utility billing theft and gas utility bill identity fraud, as well as narcotics paraphernalia and narcotics. F. 191. The SPD also discovered in that house approximately 40 LabMD day sheets, 9 copied checks payable to LabMD, and 1 money order payable to LabMD. F. 182. The day sheets found in Sacramento (the "Day Sheets"), together with the money order found in Sacramento, and the check copies found in Sacramento (the "Check Copies") are collectively referred to herein as the "Sacramento Documents," and this event is referred to herein as the "Sacramento Incident." F. 182.

The Personal Information contained in the Day Sheets consisted of names and what appear to be Social Security numbers for approximately 600 consumers. F. 183. All but two of the Day Sheets are dated between 2007 and 2008. F. 184. The remaining two Day Sheets are from March 2009. F. 184. The Check Copies contained names and bank account numbers for nine consumers, and addresses for all but one of the nine consumers. F. 185. The Check Copies are dated from May 2007 to March 2009. F. 186. The money order, dated August 2008, contained no Personal Information. F. 185, 187.

Two individuals found at the Sacramento house were arrested and charged with identity theft, receiving stolen property, possession of methamphetamine, and the possession of narcotics paraphernalia. F. 193. The Sacramento Documents were seized by the SPD and booked into evidence by the SPD. F. 195. The arrested individuals subsequently pled *nolo contendere*[35] to identity theft. F. 194.

[35] "*Nolo Contendere*" is "Latin for 'no contest.' In a criminal proceeding, a defendant may enter a plea of *nolo contendere*, in which he does not accept or deny responsibility for the charges but agrees to accept punishment. The plea differs from a guilty plea because it cannot be used against the defendant in another cause of action." Wex Legal Dictionary, published by Legal Information Institute at Cornell Law School. *See* https://law.cornell.edu/wex/nolo_contendere.

After finding the Sacramento Documents, Detective Karina Jestes of the SPD performed an Internet search and learned that the FTC was investigating LabMD. F. 209. Approximately one week after the October 5, 2012 discovery of the Sacramento Documents, Detective Jestes contacted the FTC regarding the Sacramento Documents. F. 209. In December 2012, the SPD provided the Sacramento Documents to the FTC. F. 210. The SPD made the determination not to return the Sacramento Documents to LabMD based on the FTC's investigation of LabMD. F. 210. On January 30, 2013, the FTC notified LabMD that the FTC had the Sacramento Documents. F. 211. On March 27 or 28, 2013, LabMD sent 682 letters to the consumers named in the Sacramento Documents notifying them of the Sacramento Incident, describing steps such as registering a fraud alert with credit bureaus, offering one year of free credit monitoring services, and inviting consumers to contact LabMD with questions or concerns. F. 212.

b. Summary of arguments

Relying on opinions from Mr. Kam and Mr. Van Dyke, Complaint Counsel argues that the disclosure of Personal Information for approximately 600 consumers in the Sacramento Documents is likely to cause identity theft harm. CCB at 71-72. Complaint Counsel contends that identity theft harm is likely because the types of personal information found in the Sacramento Documents, such as names and Social Security numbers on the Day Sheets, and bank routing and account numbers on the Check Copies, "can be used" by identity thieves to commit identity theft; Social Security numbers "can be used" fraudulently for extended periods of time because they are rarely changed; and there is a "likelihood" the Sacramento Documents "may have" been misused because the documents were found in the possession of individuals who later pleaded no contest to identity theft charges. CCB at 71-72. Complaint Counsel further contends, based on identity theft rates reported by the 2013 Javelin Survey, that "[c]onsumers will incur" approximately $36,000 in monetary losses from "164 cases of" NAF, ENCF, and ECF, and that "consumers will also spend 2,497 hours" resolving the resulting fraud. CCB at 72.

Respondent argues that the Sacramento Documents were found in paper form, and that Complaint Counsel has failed to prove how the documents were taken from LabMD, or how they ended up in California. Moreover, Respondent contends, there is no evidence of any consumer becoming a victim of identity theft because of the disclosure of the Sacramento Documents,

which casts doubt on Complaint Counsel's proffered expert opinions that such harm is "likely." Respondent also challenges the experts' methodology and the evidentiary bases for their opinions.

As explained below, Complaint Counsel has failed to prove that Respondent's alleged failure to reasonably secure data on its computer network caused, or is likely to cause, harm to consumers due to the exposure of the Sacramento Documents. First, Complaint Counsel has failed to prove that the Sacramento Documents were maintained on Respondent's computer network. *See* Complaint ¶ 10 (alleging Respondent failed to provide reasonable "security for personal information on its computer networks"). Second, even if there were a causal connection between Respondent's computer network and the exposure of the Sacramento Documents, the evidence fails to prove that the exposure of these documents has caused, or is likely to cause, any consumer injury.

c. Connection to LabMD's computer network

As part of its billing process, LabMD produced a report that it refers to as a "day sheet" transaction detail to ensure payments were received and posted. F. 198. Day sheets were created electronically through LabMD's billing application, Lytec. F. 199. Once day sheet reports were printed, there was no electronic record of the day sheet in LabMD's system. F. 203. Day sheets were not saved electronically. F. 203. Rather, day sheets were printed almost daily, and stored in paper files at LabMD. F. 203-204, 206. In addition, LabMD made paper copies of patient checks it received, which were retained by the billing department, and originals were shredded after six months. F. 61, 202. While the evidence shows that some LabMD day sheets and check copies may have been scanned and saved to LabMD's computer network as part of an archiving project undertaken by LabMD in or around January 2013 (F. 208), the evidence fails to show that the day sheets and copied checks *that were found in Sacramento* had been scanned and archived, or otherwise saved, onto LabMD's computer network. In fact, the Sacramento Documents were found in October 2012, months before LabMD even began to scan and archive any day sheets or check copies. F. 182, 208. These facts, combined with the fact that the Sacramento Documents were found in physical, and not electronic form (F. 197), weigh against any inference that the

Sacramento Documents were even available from Respondent's computer network, much less exposed as a result of LabMD's alleged unreasonable computer security.[36]

Complaint Counsel asserts that billing employees had "the option" of saving day sheets electronically to a computer, CCFF 156, citing deposition testimony from a former LabMD employee who worked in LabMD's billing department, identified in this Initial Decision as "the Former LabMD Employee." *See* footnote 18. However, although the Former LabMD Employee testified that the software "allowed" a user to save a day sheet or to print it, the Former LabMD employee was clear that she never saved day sheets and did not know of any LabMD employee who had saved a day sheet. F. 207. Complaint Counsel points to no evidence that any employee did electronically save any day sheets, even if it were possible to do so. In addition, although Complaint Counsel points to evidence that the SPD conducted forensic examinations of computers found in the Sacramento house where the Day Sheets and Check Copies were found, *see* CCFF 1447-1452, Complaint Counsel does not assert that these examinations found any connection to LabMD, or to LabMD's computer network.[37] In summary, the evidence upon which Complaint Counsel relies fails to prove that the Sacramento Documents were either available on, or obtained from, LabMD's computer network.

Strangely, Complaint Counsel takes no position as to how the Sacramento Documents came into the possession of the individuals in Sacramento, and further admits that "there is no conclusive explanation of how LabMD Day Sheets were exposed." CCRB at 38; *see also* Transcript of Oral Argument at 54 ("We have not presented evidence of how those documents left the possession of LabMD"); Transcript of Oral Argument at 56 ("We have -- we have made

[36] The Complaint addresses Respondent's computer network security, and does not allege that Respondent's physical security was inadequate, or that inadequate physical security constitutes an "unfair" practice under Section 5. Accordingly, Complaint Counsel's insinuation in its post-trial briefing that Respondent failed to adequately secure paper copies of the Day Sheets and Check Copies (CCRB at 38, CCFF 157-159) is outside the scope of the Complaint and, therefore, will not be considered.

[37] Evidence that a laptop seized from the Sacramento house had LimeWire installed does not prove a connection between the Sacramento Incident and LabMD's computer network. *See* CCFF 1451. The evidence shows that LabMD removed LimeWire in May 2008, and there is no contention that LimeWire or any other peer-to-peer sharing application was present on any LabMD computer after May 2008, including at the time the Sacramento Documents were discovered in October 2012. Nor is there any contention that the Sacramento Documents were at any time made available for sharing via LimeWire or another peer-to-peer application.

no representations regarding how the information left LabMD."). In related litigation between the parties, in which Respondent sought a preliminary injunction against these administrative proceedings, the district judge stated that "the FTC informed the Court that it was unaware whether the alleged identity thieves arrested in Sacramento" received the Sacramento Documents "as a consequence of LabMD's data security failures." *LabMD, Inc. v. FTC*, 2014 U.S. Dist. LEXIS 65090, at *3 n.2 (N.D. Ga. May 12, 2014); *see also LabMD, Inc. v. FTC*, No. 1:14-cv-810, Hr'g Tr. at 77, 80-81 (N.D. Ga. May 9, 2014) (cited in Respondent's motion for sanctions, filed August 14, 2014) (court exclaiming, "holy cow" in response to FTC's failure to prove chain of custody with respect to the Day Sheets).

The burden is on Complaint Counsel to prove the allegations of the Complaint that the exposure of the Sacramento Documents was caused by Respondent's alleged failure to reasonably secure its computer networks. 16 C.F.R. § 3.43(a). *See* Complaint ¶¶ 10, 21, 22. Because the evidence fails to prove that the Day Sheets and Check Copies were taken from LabMD's computer network, it would require unacceptable and unsupported speculation to conclude that the Sacramento Documents were exposed because of LabMD's alleged unreasonable computer security. Accordingly, Respondent's alleged failure to reasonably secure data on its computer network cannot properly be deemed the "cause" of any resulting harm.

Moreover, even if there were a causal connection between Respondent's alleged unreasonable data security and the exposure of the Sacramento Documents, the evidence fails to prove that the disclosure of the Sacramento Documents has resulted, or is likely to result, in any identity theft harm, as explained below.

d. Identity theft harm[38]

i. Mr. Rick Kam

(a) Opinions

Mr. Kam opined that the consumers whose Personal Information was exposed in the Sacramento Documents are "at risk of harm from identity crimes." CX0742 (Kam Expert Report at 10). Mr. Kam applied his four factor risk assessment, summarized in Section III.D.5.c., *supra*, noting that the Sacramento Documents included names, Social Security numbers, and bank account information which "could be used to commit identity theft" and that "known identity thieves" were found in the possession of the documents, which "increases the possibility that the crime occurred," notwithstanding that Detective Jestes of the SPD "could not confirm that the identity thieves used this data to commit identity fraud." CX0742 (Kam Expert Report at 22). With respect to the mitigation factor of Mr. Kam's four factor risk assessment, Mr. Kam stated that LabMD's written notification to consumers about the Sacramento Incident, offering tools such as credit monitoring, mitigated "some of the risk," but there remains a "strong possibility some of the" affected consumers will still become identity theft victims. CX0742 (Kam Expert Report at 22). Mr. Kam's opinions, summarized above, do not constitute persuasive evidence that identity theft is likely to occur as a result of the exposure of the Sacramento Documents. Mr. Kam's opinions describe little more than the possibility of future harm, or an unquantified, inchoate "risk" of future harm.

Moreover, other evidence weighs against the conclusion that the exposure of the Sacramento Documents has caused, or is likely to cause, harm. In Mr. Kam's experience with data breaches, in each case some individual has come forward to report identity theft harm, which, as Mr. Kam acknowledged, is not the case here. F. 242. Furthermore, there is no

[38] As noted in Section III.D.2.n.25, *supra*, Complaint Counsel's Post-Trial Brief and Proposed Findings of Fact do not address the likelihood of medical identity theft from the exposure of the Sacramento Documents. *See* CCB at 71-72; CCFF § 8.4. Mr. Kam's report does not contain an opinion on the likelihood of medical identity theft from the exposure of the Sacramento Documents. Mr. Van Dyke's expert report contained only a cursory opinion on the likelihood of medical identity theft generally (also referenced in Section III.D.5.d., *supra*) that "health insurance policy information and SSNs can be utilized by criminals to commit medical identity frauds . . ." CX0741 (Van Dyke Expert Report at 13). The Sacramento Documents do not contain health insurance policy information. F. 183, 185. To the extent Complaint Counsel asserts that the exposure of the Sacramento Documents is likely to cause medical identity theft harm, the evidence fails to prove that such harm has occurred, or is likely to occur.

evidence that the individuals found in possession of the Sacramento Documents had used the documents to commit identity theft prior to their arrest, and the likelihood of future misuse is reduced or eliminated by the fact that the Sacramento Documents were seized by the SPD and booked into evidence. F. 195.

In addition, Mr. Kam's opinion of the risk of harm from the exposure of the Sacramento Documents was based in part on the assertion that "approximately 100 SSNs . . . appear to have been used by people with different names," which according to Mr. Kam, "is an indicator that identity thieves may have used this information to commit identity theft." CX0742 (Kam Expert Report at 23). However, this assertion was based on an FTC staff analysis of information obtained from a Thompson Reuters Corporation (Thompson Reuters) database known as CLEAR,[39] which, as detailed below, was excluded for lack of foundation as to the authenticity and reliability of CLEAR's source data. (Tr. 372, *in camera*). For this reason as well, Mr. Kam's opinion regarding likely harm is given little weight.

(b) Exclusion of CX0451

To support Complaint Counsel's claim of identity theft harm resulting from the exposure of the Sacramento Documents, Complaint Counsel proffered a spreadsheet identified as CX0451. According to Complaint Counsel, CX0451 shows that apparent Social Security numbers appearing in connection with persons identified in the Day Sheets have been used by people with different names, which the Complaint alleges "may indicate that the SSNs have been used by identity thieves." *See* Complaint ¶ 21. Respondent objected to the admission of CX0451 on the ground, *inter alia*, of hearsay. Respondent noted that CX0451 is based upon multiple levels of hearsay; the CLEAR database, which forms the basis for CX0451, contains information from various sources that have not been substantiated; and no one had appeared from Thompson Reuters to provide a proper foundation for the reliability of the data contained in the CLEAR database. (Tr. 344, 348-351, 370, *in camera*). Complaint Counsel did not deny that CX0451 was being offered for the truth of the matter asserted, *i.e.*, that the Social Security numbers for individuals listed in the Day Sheets were being used by other individuals, implying possible

[39] CLEAR (Consolidated Lead Evaluation and Reporting) is an investigative software database program, provided by Thompson Reuters, that is used by investigators at the FTC to obtain information on individuals and corporations. F. 214.

identity theft, but maintained that CX0451 was admissible because it has "sufficient indicia of reliability to be admitted" pursuant to Rule 3.43(b). (Tr. 369, *in camera*). To address Respondent's objection, Complaint Counsel was given the opportunity to lay a foundation for the reliability of CX0451, which it sought to do through the testimony of FTC investigator Kevin Wilmer.

As set forth in detail in Section II.E.4., *supra*, Mr. Wilmer was asked by Complaint Counsel to determine whether the nine digit numbers appearing in the Sacramento Documents, which he presumed to be Social Security numbers, had been used by people with different names. F. 217-218. To perform his task, Mr. Wilmer issued a "query" to the CLEAR database. F. 219. Mr. Wilmer testified that it was his "understanding" that the CLEAR database is an aggregation of information obtained from a variety of sources, including credit bureau information, utility information, information from civil judgments and criminal convictions, and other forms of publicly and privately available information. F. 214. Specifically, Mr. Wilmer copied each number that he believed to be a Social Security number and pasted the number onto a CLEAR-provided spreadsheet. F. 219. He then submitted the spreadsheet to CLEAR with a request that CLEAR use its "batching" function to query the CLEAR database, determine who used that apparent Social Security number, and return the information to him. F. 219. In response to Mr. Wilmer's CLEAR database query, CLEAR returned a spreadsheet containing the nine digit numbers that Mr. Wilmer entered, and CLEAR's data, drawn from its various sources, as to the names of people who had used that number as a Social Security number. F. 220. Mr. Wilmer identified CX0451 as the results returned to him by Thompson Reuters in response to his CLEAR database query, to which Mr. Wilmer added certain color-coding to differentiate the various names. F. 221.

After viewing proffered CX0451, hearing testimony from Mr. Wilmer, and considering the arguments of the parties, admission of CX0451 was denied on the ground that there was an insufficient foundation for determining the accuracy or reliability of the information in the CLEAR database, which provided the data for proffered CX0451. The ruling stated preliminarily: "I have concerns and I continue to have concerns about the reliability of the data comprising the spreadsheet [CX0451]. For example, I ruled earlier in this trial that I wouldn't allow sworn affidavits to be admitted into evidence. In this case, we are lacking even a sworn

statement or certification that the . . . CLEAR data is in fact accurate. And in fact, I have no idea if there's a . . . disclaimer on the Website stating that the information is not accurate." (Tr. 371, *in camera*). The ruling concluded that the foundation laid by Complaint Counsel was "wholly and totally lacking to make [CX0451] sufficiently reliable" to show that apparent Social Security numbers in the Sacramento Documents are being used by other people and therefore indicative of identity theft having occurred in this case. *See also* Tr. 371-372, *in camera* ("[W]e don't know if the Social Security number on the day sheet was correct [and w]e don't know if the Social Security number that the CLEAR data reflected was accurate. . . . [T]he source of [the CLEAR database] is from so many varied areas, real estate documents, utility bills, law enforcement records, criminal indictments, whatever, someone could easily type incorrectly one of the digits of a Social Security number.").

The record amply supports the denial of admission of proffered CX0451 as probative evidence of potential or actual identity theft from the exposure of the Sacramento Documents. The reliability of proffered CX0451 turns on the authenticity, accuracy, and/or reliability of the CLEAR database, and specifically, the data that is entered into the public and private databases from which the CLEAR database draws its information. However, Mr. Wilmer lacked sufficient knowledge of these matters. F. 224-226. In fact, Mr. Wilmer could not possibly authenticate or otherwise vouch for the reliability of the data in CX0451 since he has no personal knowledge of the CLEAR database itself, or the accuracy or reliability of the source data comprising the CLEAR database. F. 224-226. In addition, Mr. Wilmer, who had no connection to Thompson Reuters, which collects the source data upon which CX0451 is based, did not ask CLEAR to identify the source(s) of the data CLEAR used to populate the CLEAR spreadsheet, although he could have received this information if he had asked, because "that wasn't a part of [his] assignment." F. 224. Mr. Wilmer had no knowledge of, and did not ask CLEAR, whether some of the numbers reported by CLEAR had stemmed from bad keystrokes on the part of a reporting source, such as a bank. F. 225. Mr. Wilmer was not asked to determine any of the above, and was not asked to, and did not, contact any of the individuals listed in the Sacramento Documents. F. 226. In fact, Mr. Wilmer was not even asked to confirm that the nine digit numbers appearing on the Day Sheets in fact constituted Social Security numbers, or that the presumed Social Security numbers actually belonged to the associated names in the Sacramento Documents.

F. 217-218, 222. The spreadsheet offered as CX0451 does not indicate which individual associated with a Social Security number is the true owner of the number, if any.[40] F. 223.

Based on the failure to demonstrate the authenticity or reliability of the data returned by the CLEAR database, which is contained in proffered CX0451, the document cannot properly support any factual finding or any valid conclusion in this case. Moreover, even if proffered CX0451 were sufficiently reliable to be admitted, at best, proffered CX0451 shows only that individuals with different names are using the same Social Security number. However, on the record presented, this fact does not demonstrate or even imply that consumers in the Sacramento Documents are victims of identity theft. As noted above, there is no evidence that the individuals associated with Social Security numbers in the Sacramento Documents are the true owners of those Social Security numbers, and this fact cannot properly be assumed. Moreover, the evidence fails to show whether or not some of the people listed in the Sacramento Documents had voluntarily shared their personal information for others to use, or whether family members had taken their personal information without consent.

For all the foregoing reasons, Complaint Counsel has failed to prove the allegation in Complaint ¶ 21 that Social Security numbers in the Sacramento Documents "are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves," and Mr. Kam's opinions of likely identity theft from the Sacramento Documents, to the extent they rely on the assertion that Social Security numbers in the Sacramento Documents have been used by people with different names, are entitled to no weight.

ii. Mr. James Van Dyke

In support of its claim that the exposure of the Sacramento Documents is likely to cause substantial consumer injury, Complaint Counsel also relies on statistics reported in the 2013 Javelin Survey, also referenced in Section III.D.5.c.ii., *supra* regarding the 1718 File, that

[40] Indeed, even the relevance of CX0451 is questionable since Complaint Counsel failed to prove that the Sacramento Documents were even connected to Respondent's computer network security as alleged in the Complaint.

(1) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing new account fraud within the preceding 12 months, at an average consumer loss of $449; (2) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing existing non-card fraud within the preceding 12 months, at an average consumer loss of $207; and (3) 13.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing existing card fraud with the preceding 12 months, at an average consumer cost of $106. CX0741 (Van Dyke Expert Report at 8-12). This evidence is unpersuasive, however. Mr. Van Dyke did not conduct a survey of the consumers listed in the Sacramento Documents. F. 256. The consumers whose Social Security numbers were exposed in the Sacramento Incident were notified of the incident in March 2013. F.212. If the assumptions underlying Complaint Counsel's theory of likely harm were to be believed and applied to this incident, then at least some of these consumers would have become victims of identity theft within 12 months. Yet, Complaint Counsel fails to identify even one consumer who suffered identify theft or identity fraud, within that 12 month period, or at any time thereafter. These facts undermine the persuasive value of Mr. Van Dyke's opinions and the assertion that harm is likely in this case.

e. Conclusion

For all the foregoing reasons, the evidence fails to prove that Respondent's alleged failure to reasonably secure the data on its computer network caused the exposure of the Sacramento Documents, or that this exposure has caused, or is likely to cause, substantial consumer harm.

7. Risk of Harm to Consumers whose Personal Information is Maintained on LabMD's Computer Network

a. Introduction

Complaint Counsel argues that LabMD's alleged failure to employ reasonable security practices "placed all consumers whose Personal Information is on [LabMD's computer] network at risk." CCB at 68. In support of this contention, Complaint Counsel points to opinions of its experts that the types of personal data kept by LabMD, such as names, Social Security numbers,

payment information, and health insurance information, "are the types of information needed to perpetrate frauds, and are the target of data thieves." CCB at 68. Therefore, Complaint Counsel concludes, the "risk of unauthorized exposure . . . is likely to cause" identity theft, medical identity theft, and other harms. CCB at 68. Put another way, Complaint Counsel argues that Respondent's alleged unreasonable data security creates an "elevated" or "increased" risk of an unauthorized disclosure, and that there is a "correlation" between being a data breach victim and being an identity theft victim; therefore, Respondent's alleged unreasonable data security is "likely to cause" consumers harm. CCCL 27.

Respondent contends that Complaint Counsel's position, based upon expert opinion, constitutes speculation about possible future identity theft, while the record is devoid of evidence of actual or likely identity theft, and does not satisfy Complaint Counsel's burden under Section 5(n) to prove that Respondent's alleged conduct caused or is likely to cause substantial consumer injury. Respondent further argues that Complaint Counsel's proffered consumer injury experts were not qualified to assess the risk posed by Respondent's alleged unreasonable data security, and that their opinions as to risk were based on assumptions and speculation.

As explained further below, Complaint Counsel's theory that harm is likely for all consumers whose Personal Information is maintained on LabMD's computer network, based on a "risk" of a future data breach and resulting identity theft injury, is without merit. First, the expert opinions upon which Complaint Counsel relies do not specify the degree of risk posed by Respondent's alleged unreasonable data security, or otherwise assess the probability that harm will result. To find "likely" injury on the basis of theoretical, unspecified "risk" that a data breach will occur in the future, with resulting identity theft harm, would require reliance upon a series of unsupported assumptions and conjecture. Second, a "risk" of harm is inherent in the notion of "unreasonable" conduct. To allow unfair conduct liability to be based on a mere "risk" of harm alone, without regard to the probability that such harm will occur, would effectively allow unfair conduct liability to be imposed upon proof of unreasonable data security alone. Such a holding would render the requirement of "likely" harm in Section 5(n) superfluous, and would contravene the clear intent of Section 5(n) to limit unfair conduct liability to cases of actual, or "likely," consumer harm.

b. Analysis

As framed by Complaint Counsel, the likelihood of substantial consumer injury to the consumers whose Personal Information is presently maintained on Respondent's computer network is based on the asserted risk that identity thieves, targeting the types of information held by LabMD, will successfully breach Respondent's computer network, take Personal Information, and misuse that information to commit identity theft harms. In the instant case, there is no evidence that this has happened in the past,[41] or that any consumer has suffered any harm as a result of Respondent's alleged unreasonable data security, including as a result of the alleged Security Incidents, as discussed above.

In *International Harvester*, upon which Complaint Counsel relies on the issue of risk (*see* CCCL 26), the Commission was required to assess the risk of consumer harm from certain safety defects in the respondent's tractors, to determine whether it was deceptive to fail to disclose such defects. "The implied warranty of fitness is not violated by all undisclosed safety problems. The critical issue is the degree of risk involved. . . . [A] seller impliedly warrants only that a product is reasonably safe, not that it is free of all hazards. We recognize that there is no such thing as a totally safe product, and especially not when dealing with relatively complex machinery." 1984 FTC LEXIS 2, at *252 and n.50. Similarly, as the Commission has acknowledged in this case, "[t]here is no such thing as perfect [computer] security." *LabMD*, 2014 FTC LEXIS 2, at *52. Accordingly, it was incumbent upon Complaint Counsel to demonstrate "the degree of risk involved." *See Int'l Harvester*, 1984 FTC LEXIS 2, at *252 and n.50. As the Commission stated in *International Harvester*, to suggest that there is a kind of risk that is separate from statistical risk "amounts really to no more than a conversational use of the term in the sense of 'at risk.' In this sense everyone is 'at risk' at every moment, with respect to every danger which may possibly occur. When divorced from any measure of the probability of occurrence,

[41] As noted above in Section III.D.6., the evidence fails to prove that the Sacramento Documents were obtained from a breach of Respondent's computer network security. In addition, as discussed above in Section III.D.5., while the 1718 File incident constituted a "data breach" in the broad sense of an unauthorized disclosure, the circumstances under which that disclosure occurred, through Tiversa's locating and downloading the 1718 File via peer-to-peer file sharing, are not analogous to the type of targeted intrusion of computer security by identity thieves posited by Complaint Counsel.

however, such a concept cannot lead to useable rules of liability." *Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52.[42]

Judged against the principles for assessing risk set forth in *International Harvester*, the opinions of Complaint Counsel's experts, upon which Complaint Counsel relies, are insufficient because the experts failed to specify the degree of risk, or otherwise measure the probability or likelihood that Respondent's alleged unreasonable data security will result in a data breach and identity theft injury. Mr. Kam opined generally that Respondent's asserted failure to reasonably protect its consumers' Personal Information poses an "increased" or "elevated" risk of unauthorized disclosure of this information, which "in turn is likely to cause" identity theft harm. CX0742 (Kam Expert Report at 10, 23). He based this opinion on the further broad opinion that cyber-criminals in general target healthcare organizations for attack, and that inadequate data security by such organizations renders their data security systems "vulnerable" to an attack by these criminals. *Id.* at 23; *see also* Kam, Tr. 558. *See* CCFF 1646-1649; 1653-1656. Mr. Kam "assumed" that Respondent's data security was unreasonable, and did not undertake to assess the degree of risk presented by Respondent's particular practices, or to assess the probability or likelihood that Respondent's computer network will be breached in the future. F. 244-245. Indeed, Mr. Kam has no expertise in computer network security, and therefore could not properly opine on the risk posed by Respondent's computer security, or on the probability or likelihood of a breach. *See* F. 9-10, 245. Mr. Kam's opinions as to a generalized increased risk of cyber-attack on healthcare organizations whose data security systems are "vulnerable" to such criminals is "divorced from any measure of the probability" of such an occurrence in this case. *See Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. Accordingly, Mr. Kam's opinion in this regard is not persuasive evidence that any or all the consumers whose Personal Information is maintained by LabMD on its computer network are "likely" to suffer harm.

The opinion offered by Complaint Counsel's other consumer harm expert, Mr. Van Dyke, also fails to assess the probability or likelihood that Respondent's alleged unreasonable data security will result in a data breach and resulting harm. Mr. Van Dyke candidly admitted

[42] As noted above, as in *International Harvester,* risk is a critical issue for Complaint Counsel's claim. Accordingly, notwithstanding that the discussion of risk in *International Harvester* was in the context of a deception claim, as opposed to an unfair conduct claim, the Commission's framework for assessing risk is nevertheless instructive.

that he did not, and was not able to, provide any quantification of the risk of identity theft harm for the 750,000 consumers whose information is maintained on LabMD's computer networks, because he did not have evidence of any data exposure with respect to those individuals, except as to those that were listed on the 1718 File or in the Sacramento Documents. F. 258.

Moreover, Mr. Van Dyke's "risk" opinion is even more amorphous than that of Mr. Kam. Mr. Van Dyke states that, because consumer personal information in general is a "target of data thieves," LabMD's alleged unreasonable data security "risked exposing" consumers "to a likelihood" of harm. CX0741 (Van Dyke Expert Report at 12-13). Whatever the meaning of "likely" harm, as used in Section 5(n), surely it requires more than a mere "risk" of "an exposure" to "a likelihood" of harm. *See also* CCCL 30 (arguing that in "potentially exposing" consumers' Personal Information "to unauthorized disclosure," Respondent's conduct is "likely to cause injury . . .").

Furthermore, like Mr. Kam, Mr. Van Dyke did not assess Respondent's particular data security practices, having assumed that Respondent's data security was "unreasonable," F. 257, and his opinion is therefore also "divorced from any measure of the probability" that a data breach, and resulting identity theft harm, will occur in this case. *See Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. In addition, like Mr. Kam, Mr. Van Dyke is not qualified to assess Respondent's computer security. *See* F. 12-14.

The only expert proffered by Complaint Counsel who is arguably qualified to assess the degree of risk posed by Respondent's computer security practices, Dr. Raquel Hill, did not opine as to the probability or likelihood that Respondent's computer network would be breached, or whether Respondent's data security practices were likely to cause any consumer harm. When asked if she had an opinion as to the likelihood of consumer harm resulting from Respondent's asserted unreasonable data security, Dr. Hill responded that she did not form such an opinion; that she was instructed to assume that identity theft harm "could occur" *if* consumers' personal information on LabMD's network was exposed; and that she "assumed" that such harm was likely. F. 237. The likelihood of such an exposure, and resulting consumer harm, cannot properly be assumed. This assumption by the government's only witness who arguably could have opined on the specific risk or probability that Respondent's particular data security

practices will result in an unauthorized exposure – the logical prerequisite to any potential consumer harm – leaves virtually no evidence to support the contention that LabMD's alleged unreasonable security practices are likely to cause harm to consumers, simply because their Personal Information is maintained on Respondent's computer network.

Under the evidence presented, to conclude that consumers whose Personal Information is maintained on Respondent's computer network are "likely" to suffer a data breach and subsequent identity theft harm would require speculation upon speculation. Among other things, it would have to be assumed that, at some unknown point in the future, Respondent's computer system will be breached by a presently unknown third-party who, at some undetermined point thereafter, will use the stolen information to harm those consumers.[43] *Cf. Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3rd Cir. 2011) (finding alleged increased risk of future injury too attenuated for Article III standing purposes, even though there had been a prior security breach by an unknown hacker, because the likelihood of actual injury from the breach was "dependent on entirely speculative, future actions of an unknown third-party"). *See* Policy Statement, *supra*, at *307 (stating that injury must not be speculative); 1982 Policy Letter, *supra* (stating that Commission's resources should not be used for speculative harm).

Moreover, if an unspecified, theoretical "risk" of a future data breach and resulting identity theft were sufficient to prove unfair conduct in the instant case, then the clear requirement in Section 5(n) that injury be "likely" would be vitiated. Under common law negligence principles, which both parties cite in connection with the meaning of "unreasonableness" (CCCL 16; RCL 97),[44] "unreasonable" conduct, by definition, is conduct

[43] Complaint Counsel's argument as to the likelihood of future harm for all consumers whose Personal Information is maintained by LabMD is premised on the asserted vulnerability of LabMD's computer network to infiltration by identity thieves who would then commit identity crimes. To the extent Complaint Counsel also argues a likelihood of emotional or other privacy harms, allegedly arising from an unauthorized exposure of sensitive medical information alone, such subjective harm, unaccompanied by any tangible injury such as monetary harm or health and safety risks, would not constitute "substantial injury" within the meaning of Section 5(n).

[44] The Commission also referred to negligence standards as relevant to the "unreasonable data security" claim in the instant case. *LabMD*, 2014 FTC LEXIS 2, at *47-48. In rejecting LabMD's contention that charging LabMD with employing unreasonable data security in the absence of promulgated data security standards violated due process, the Commission stated: "LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself."

that exposes another to an unreasonable "risk" of harm. *See, e.g.*, Restatement (Second) of Torts § 298 (reasonable conduct is that which a reasonable person would recognize as necessary to prevent creating an unreasonable risk of harm); *see also id.* at § 291 ("Where an act is one which a reasonable man would recognize as involving a risk of harm to another, the risk is unreasonable and the act is negligent if the risk is of such magnitude as to outweigh what the law regards as the utility of the act or of the particular manner in which it is done."). Thus, to contend that proof of risk of injury – even an elevated or increased risk – is sufficient to prove "unfair" conduct is tantamount to arguing that "unreasonable" data security, by definition, is an unfair practice. This is contrary to the theory of the Complaint, which alleges both unreasonable data security and likely injury. Complaint ¶¶ 10, 22. *See also LabMD*, 2014 FTC LEXIS 2, at *52 (holding that unfair conduct liability in the area of data security requires proof of unreasonable data security *and* actual or likely resulting injury) (emphasis added). In addition, to base unfair conduct liability upon proof of unreasonable data security alone would, on the evidence presented in this case, effectively expand liability to cases involving generalized or theoretical "risks" of future injury, in clear contravention of Congress' intent, in enacting Section 5(n), to limit liability for unfair conduct to cases of actual or "likely" substantial consumer injury. *See, e.g.*, H.R. CONF. REP. 103-617, 1994 WL 385368, at *11-12, FTC Act Amendments of 1994 (noting that Section 5(n) is to *limit* unfair acts or practices under the reach of Section 5 to those that, *inter alia*, "cause or are likely to cause substantial injury to consumers") (emphasis added); *see also* S. REP. 103-130, 1993 WL 322671, at *4 ("This section amends section 5 of the FTC Act to limit unlawful 'unfair acts or practices' to *only* those which cause or are likely to cause substantial injury to consumers . . .") (emphasis added).

It is also significant that the Commission, in rejecting Respondent's argument that the unfair conduct claim in this case violated its due process rights to fair notice of what conduct was prohibited, specifically held that "the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n)," provided the required constitutional notice. *LabMD*, 2014 FTC LEXIS 2, at *46. That three-part statutory standard prohibits conduct that, *inter alia*, "causes or is likely to cause" substantial consumer injury. If unfair conduct liability can be premised on "unreasonable" data security alone, upon proof of a generalized, unspecified "risk" of a future data breach, without regard to the probability of its occurrence, and without

proof of actual or likely substantial consumer injury, then "the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n)," would not provide the required constitutional notice of what is prohibited.

Complaint Counsel asserts that Section 5 unfair conduct liability can be imposed based solely on the risk of a data breach and that proof of an actual data breach is not required. Transcript of Closing Arguments, Sept. 16, 2015, at 57. Fundamental fairness dictates that proof of likely substantial consumer injury under Section 5(n) requires proof of something more than an unspecified and hypothetical "risk" of future harm, as has been submitted in this case.[45]

c. Conclusion

Proof of a "risk" of harm, alone, "[w]hen divorced from any measure of the probability of occurrence, . . . cannot lead to useable rules of liability." *Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. In the instant case, at best, Complaint Counsel's evidence of "risk" shows that a future data breach is possible, and that if such possible data breach were to occur, it is possible that identity theft harm would result. However, possible does not mean likely. Possible simply means not impossible. Such proof does not meet the minimum standard for declaring conduct "unfair" under Section 5 of the FTC Act, which requires that harm be "likely," and cannot lead to useable rules of liability. Accordingly, for all the foregoing reasons, the evidence fails to prove that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial injury to consumers whose Personal Information is maintained on LabMD's computer network.

E. CONCLUSION

Section 5(n) of the FTC Act provides that "[t]he Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the

[45] It should also be noted that Complaint Counsel's proffered data security expert, Dr. Hill, confined her opinions as to Respondent's alleged unreasonable data security to the time period from January 2005 through July 2010, referred to as the "Relevant Time Period." Thus, whatever risk might be inherent in Respondent's alleged "unreasonable" data security during the Relevant Time Period, the record is devoid of expert opinion as to the degree of risk beyond that period. Also, relevant to the assessment of risk in this case is that LabMD wound down its operations beginning in January 2014, and, as of May 2014, LabMD's operations were limited to maintaining tissue samples, and providing copies of prior test data to its physician clients only via facsimile. F. 36-39.

act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Accordingly, in the instant case, the burden was on Complaint Counsel to prove, initially, that Respondent's alleged failure to employ "reasonable and appropriate" data security "caused, or is likely to cause, substantial injury to consumers," as alleged in the Complaint. Complaint ¶¶ 10, 22. The evidence presented in this case fails to prove these allegations. As addressed in detail in this Initial Decision, there is no evidence that any consumer has suffered any substantial injury as a result of Respondent's alleged conduct, and both the quality and quantity of Complaint Counsel's evidence submitted to prove that such injury is, nevertheless, "likely" is unpersuasive. In reaching these conclusions the totality of the record evidence has been fully considered and weighed.

In summary, there is no evidence that any consumer has suffered any injury as a result of the 2008 exposure of the 1718 File, and the evidence fails to show that this exposure, to Tiversa, Professor Johnson, and the FTC, is likely to cause any substantial consumer injury. In addition, the evidence further fails to show that the Sacramento Documents were exposed in 2012 as a result of any alleged computer security failure of Respondent, or that the exposure of these documents has caused, or is likely to cause, any substantial consumer injury. Finally, the theory that, there is a likelihood of substantial injury for all consumers whose information is maintained on Respondent's computer networks, because there is a "risk" of a future data breach, is without merit because the evidence presented fails to demonstrate a likelihood that Respondent's computer network will be breached in the future and cause substantial consumer injury. While there may be proof of possible consumer harm, the evidence fails to demonstrate probable, *i.e.*, likely, substantial consumer injury.

Because the evidence fails to prove that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury, as required by Section 5(n) of the FTC Act, Respondent's alleged unreasonable data security cannot properly be declared an unfair act or practice in violation of Section 5(a) of the FTC Act. Accordingly, the Complaint must be DISMISSED.

IV. SUMMARY OF CONCLUSIONS OF LAW

1. Section 5 of the FTC Act grants the FTC the authority over "unfair or deceptive acts or practices in or affecting commerce" by "persons, partnerships, or corporations . . . ." 15 U.S.C. § 45(a)(1)-(2).

2. Respondent is a corporation within the meaning of Sections 4 and 5 of the FTC Act. 15 U.S.C. §§ 44, 45.

3. The acts and practices alleged in the Complaint are "in or affecting commerce" under the FTC Act. 15 U.S.C. § 45(a)(1).

4. Complaint Counsel bears the burden of proving the allegations of the Complaint that Respondent engaged in unfair conduct in violation of Section 5(a) of the FTC Act by a preponderance of evidence.

5. Section 5(n) of the FTC Act provides that "[t]he Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

6. Complaint Counsel bears the burden of proving by a preponderance of the evidence the allegations of the Complaint that Respondent's failure to provide "reasonable and appropriate" security for personal information maintained on LabMD's computer networks, "caused or is likely to cause" substantial consumer injury that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

7. Congress amended the FTC Act in 1994 to add Section 5(n). Congress' intent in adding Section 5(n) to the FTC Act was to establish an outer limit to the Commission's authority to declare an act or practice unfair.

8. Section 5(n) of the FTC Act is a three-part test, and all three parts must be proven before an act or practice can be declared "unfair."

9. The three-part test in Section 5(n) was intended to codify, as a statutory limitation on unfair acts or practices, the principles of the FTC's December 17, 1980 policy statement on unfairness, reaffirmed by a letter from the FTC dated March 5, 1982, in order to provide guidance and to prevent a future FTC from abandoning those principles.

10. Actual or likely substantial consumer injury, which is also not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to

consumers or to competition, is a legal precondition to finding a respondent liable for unfair conduct.

11. Unjustified consumer injury is the primary focus of the FTC Act.

12. The Commission has stated that its "concerns should be with substantial consumer injuries; its resources should not be used for trivial or speculative harm."

13. Consumer injury may be "substantial" under Section 5(n) if a relatively small harm is inflicted on a large number of consumers or if a greater harm is inflicted on a relatively small number of consumers.

14. In most cases, substantial consumer injury involves monetary or economic harm or unwarranted health and safety risks.

15. Unfair conduct cases usually involve actual and completed harms.

16. Historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm.

17. Complaint Counsel bears the burden of proving, initially, that Respondent's alleged failure to employ "reasonable and appropriate" data security "caused, or is likely to cause, substantial injury to consumers," as alleged in the Complaint.

18. Complaint Counsel has failed to meet its burden of proving that Respondent's alleged unreasonable data security caused substantial consumer injury. The record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged conduct.

19. Section 5(n) does not define the meaning of "likely" injury. Where a statute does not define a term, it is construed in accordance with its ordinary meaning.

20. The Merriam-Webster dictionary states that "likely" is "used to indicate the chance that something will happen," and is primarily defined as "having a high probability of occurring or being true."

21. The Commission has interpreted its deception standard, which requires proof that a practice is "likely to mislead" consumers, to require proof that such deception was "probable, not possible . . . ."

22. The term "likely" in Section 5(n) does not mean that something is merely possible. Instead, "likely" means that it is probable that something will occur.

23. Complaint Counsel has failed to meet its burden of proving that Respondent's alleged unreasonable data security is "likely to cause" substantial consumer injury. There

may be proof of possible consumer harm, but the evidence fails to demonstrate probable, *i.e.*, likely, substantial consumer injury.

24. Complaint Counsel has failed to prove that the 2008 exposure of the 1718 File caused, or is likely to cause, any substantial consumer injury.

25. Subjective feelings of harm, such as embarrassment, upset, or stigma, standing alone, without accompanying, clearly demonstrated, tangible injury, do not constitute "substantial injury" within the meaning of Section 5(n).

26. Evidence in the record provided by Tiversa and its chief executive officer and corporate designee Mr. Robert Boback, claiming that Tiversa found the 1718 File in "multiple locations" on peer-to-peer networks, including at IP addresses belonging to suspected or known identity thieves, is entitled to no weight. Such evidence, including without limitation, Mr. Boback's 2013 discovery deposition, Mr. Boback's 2014 trial deposition testimony, and a Tiversa-provided exhibit, CX0019, is unreliable, not credible, and outweighed by credible contrary testimony from Mr. Richard Wallace.

27. Complaint Counsel has failed to prove that Respondent's alleged failure to reasonably secure data on its computer network caused, or is likely to cause, substantial injury to consumers due to the exposure of the Sacramento Documents because Complaint Counsel has failed to prove that the Sacramento Documents were maintained on Respondent's computer network.

28. Complaint Counsel has failed to prove that the Sacramento Documents were exposed in 2012 as a result of any alleged computer security failure of Respondent.

29. Even if there were a causal connection between Respondent's computer network and the exposure of the Sacramento Documents, Complaint Counsel has failed to prove that the exposure of these documents has caused, or is likely to cause, any substantial consumer injury.

30. Complaint Counsel has failed to prove the allegation in Complaint ¶ 21 that Social Security numbers in the Sacramento Documents "are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves," because the evidence upon which Complaint Counsel relies (proffered exhibit CX0451) is unreliable and entitled to no weight.

31. Complaint Counsel's assertion that there is a likelihood of substantial injury for all consumers whose information is maintained on Respondent's computer networks, regardless of whether their information has been exposed, on the theory that there is a "risk" of a future data breach, is without merit because Complaint Counsel has failed to prove the likelihood that Respondent's computer network will be breached in the future and cause substantial consumer injury.

32. To suggest that there is a kind of risk that is separate from statistical risk amounts to no more than a conversational use of the term "risk." Proof of a "risk" of harm alone, when divorced from any measure of the probability of occurrence, cannot lead to useable rules of liability.

33. To find "likely" substantial consumer injury on the basis of theoretical, unspecified "risk" that a data breach will occur in the future, with resulting identity theft harm, would require reliance upon a series of unsupported assumptions and conjecture.

34. To allow unfair conduct liability to be based on proof of a generalized "risk" of harm alone – even an elevated or increased risk – without regard to the probability that such harm will occur would vitiate the requirement in Section 5(n) that substantial consumer injury be proven "likely" and would contravene the clear intent of Section 5(n) to limit unfair conduct liability to cases of actual, or "likely," substantial consumer injury.

35. Proof of likely substantial consumer injury under Section 5(n) requires proof of something more than an unspecified and hypothetical "risk" of future harm.

36. Based on the totality of the evidence presented, Complaint Counsel has failed to meet its burden of proving, by a preponderance of the evidence, that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury.

37. Because Complaint Counsel failed to meet its burden of proving the first prong of the three-part test in Section 5(n) – that Respondent's conduct caused, or is likely to cause, substantial consumer injury – Respondent's alleged failure to employ "reasonable and appropriate data security" for information maintained on its computer networks cannot be declared an "unfair" act or practice in violation of Section 5(a) of the FTC Act.

ORDER

For the reasons stated above, IT IS ORDERED that the Complaint be, and hereby is, DISMISSED.

ORDERED:

_____

D. Michael Chappell
Chief Administrative Law Judge

Date: November 13, 2015