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

TABLE OF CONTENTS

I. INTRODUCTION

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,

Commission's Rules of Practice, the Motion was decided by the Commission[1] Å 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,

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

d

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,e36-2(i)-2(t)begarnto iunervlo

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

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 r -0.002 TeT9y3 Tw [n 0.002-10(y)20(puom]/BB)4(nj /TT14174.639 0f0(3 Two)2( )2-10(y]TJ

assertions made on page 49 of Complaint Counsel's pre-trial brief are not repeated

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"

7. Dr. Hill's conclusions in this case are limited to

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

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, ates of birth, Social Sec

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 I

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 av

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 inst6(a)6(s)]TJ 08a beeons of 6(ad)74(bl)-2(e)4l(d t)-2(ha4(ont)5 LA03 Tw 9.49 0 Td ()1(n M)-11(9)]TJ Tw 18.05 0 Td ( ).09(t)-2(h)-10(ID 26 >>BDC -17321 -1.15

104.

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.

"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

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 RX 645, 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

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

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 p(ll)-1018(g)1l3 -0.ga-11(e)4(.h418(g)Tj EMC /LBody <</4(hn2(d)2mila(in)2(n)2(a)2(n)2(tn)2(a(

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

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 d share a couple0(y)20(f)-7(ilA)2(pr)3(i)-2(2boo-6(r)3(s)-1.fo-2(c)4(as)1(o)2(me)6(in)2(te)6(6(Yimp4

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

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)).

198. As part of its

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 ofthe 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

235. As a matter of common usage, the generic term “identity theft” may include “identity

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-

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 adults4[d4

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

C.

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 explegedly that,-2(o ( )e)4(f)3(u)-1 a020tiibt u12c-2(de(e)4(n

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

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 H arm

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/a. Tc 0P <</Mm

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

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/

challenged conduct is “likely” to cause harm in the future. Moreover, although some courts have

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

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,

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

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.

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

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

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 undermieTd [(-d [(-I22(y)TT1 1

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.

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 S

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 con.32 0 Td (;)Tjn the poss33003 Tc 0.003 2 (")Tj (nt)-2(o D)2(oc)4w(;)Ti8.72 opi hhe

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 representatio

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 er -1(s)-ow

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 Ssa(a)hm

statement or certification that the . . .

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

(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,

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

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,"

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

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

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 d(nd bot)-2(h td(nd ul)-2(l)-12(ye)4(S

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.

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.

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 emplo" 5ntntialf ( )Tj ( )-3(e