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

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

OPPOSITION TO MOTION TO DISMISS

The Court should deny Respondent's Motion to Dismiss because it fundamentally misconstrues the law of unfairness under Section 5 of the Federal Trade Commission Act ("FTC Act"). Respondent incorrectly argues that to establish unfairness Complaint Counsel must prove that LabMD's unreasonable data security practices resulted in the exposure of the 1718 File and the Day Sheets and that these two specific incidents harmed consumers.

Section 5 expressly states that an act or practice is unfair where it "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) (emphasis added). Respondent focuses on the first element of unfairness.[1] Contrary to Respondent's assertions, however, unfairness does not require Complaint Counsel to identify a particular disclosure incident resulting from Respondent's systemic data security failures or to show that a specific consumer has already been harmed. Although indicative that

[1] Respondent's motion does not address the "not reasonably avoidable" and "not outweighed by countervailing benefits" elements of the unfairness test. Therefore, Complaint Counsel does not address them in this Opposition.

LabMD's security failures were likely to cause consumer harm, Complaint Counsel does not need to identify particular data breaches in order to prove its case. Moreover, even though in this case numerous consumers may have already suffered substantial injury as a result of Respondent's unreasonable practices, the unfairness standard does not require the Commission to wait until harm occurs before taking action to protect consumers.[2]

To establish a *prima facie* case on the likelihood of injury element of unfairness, Complaint Counsel must show that Respondent's unreasonable data security practices were likely to result in unauthorized exposure of data, and that exposure of the sensitive Personal Information that LabMD maintains is likely to cause substantial consumer injury. Complaint Counsel has met this burden.

BACKGROUND

The hearing in this matter commenced on May 20, 2014. In addition to the documentary evidence presented to the Court before commencement of the hearing – *see, e.g.*, JX0002 (Joint Stipulation on Admissibility of Exhibits) (identifying witness trascripts and exhibits received by the Court as evidence in this matter) – Complaint Counsel presented the testimony of its affirmative experts, Dr. Raquel Hill (information security practices), James Van Dyke (consumer harm), and Rick Kam (consumer harm), on May 20th through 23rd and then rested its case.[3] Respondent thereafter submitted this motion.

---

[2] 15 U.S.C. § 45(n). *Cf. FTC v. Toysmart.com LLC*, No. 00-11341 (D. Mass. July 21, 2000), available at http://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc (consent order) (requiring bankrupt company that intended to sell consumers' Personal Information in violation of its privacy policy representations to delete such Personal Information rather than sell it).

[3] After resting, Complaint Counsel called its expert witness in rebuttal, Dr. Clay Shields (peer-to-peer file-sharing).

ARGUMENT

I. LEGAL STANDARD FOR UNFAIRNESS

Section 5 unfairness requires Complaint Counsel to prove that Respondent's practices "[1] cause[d] or [are] likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Rule 3.43(a) states that "Counsel representing the Commission . . . shall have the burden of proof," except as to factual propositions put forward by another proponent, such as affirmative defenses. *See also* Administrative Procedure Act, 5 U.S.C. § 556(d). The standard of proof is preponderance of the evidence. *In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *133-35 (Aug. 5, 2009) (collecting cases).

Congress deliberately delegated broad power to the FTC under Section 5 of the FTC Act to address unanticipated practices in a changing economy. *See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972). Among the other practices from which it protects consumers, unfairness encompasses unreasonable data security. Comm'n Order on Resp't's Mot. to Dismiss at 3; *FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *9 (D.N.J. Apr. 7, 2014). Applied to data security, the unfairness analysis begins with an assessment of consumer injuries that may result from a company's information security practices. As the Commission has made clear, a showing of substantial injury or the likelihood of substantial injury from a company's security practices does not require that an actual breach occur. *See* Comm'n Order on Resp't's Mot. to Dismiss at 19 ("[O]ccurrences of actual data security breaches or 'actual, completed economic harms' are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted 'unfair . . . acts or practices.") (citations omitted). Instead, this inquiry turns on whether the company's security

practices caused or are likely to cause consumer harm. *Id.* at 18-19 (requiring assessment of whether a company's "data security procedures were 'unreasonable' in light of the circumstances"). The second consideration is whether consumers could have avoided this harm. *Id.* at 19. Finally, even if the security practices cause or are likely to cause harm to consumers that is unavoidable, unfairness requires assessing whether the unreasonable security practices benefit consumers or competition. *Id.* Countervailing benefits of maintaining unreasonable security are unlikely to be significant when the cost of more effective security measures is relatively low. As the Commission recently expressed it: "the touchstone of the Commission's approach to data security is reasonableness." Comm'n Statement Marking 50th Data Sec. Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Comm'n Order on Mot. to Dismiss at 8 (Commission has authority "to take action against unreasonable data security measures as 'unfair . . . acts or practices' in violation of Section 5").

As with the application of the reasonableness standard of care in any other circumstance, what constitutes reasonable data security practices for a company that maintains consumers' sensitive personal information will vary depending on the circumstances. *See FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) ("[T]he proscriptions in [Section] 5 are flexible, 'to be defined with particularity by the myriad of cases from the field of business.'") (internal citations omitted); *Brock v. Teamsters Local Union No. 863*, 113 F.R.D. 32, 34 (D.N.J. 1986) (reasonableness under prudent man standard "tried on the individual facts of [the] case" in light of standards developed in case law); *In re Zappos.com, Inc.*, No. 12-00325, 2013 WL 4830497, at *3-4) (D. Nev. Sept. 9, 2013) (applying "reasonable and prudent person" standard in negligence case for failure to safeguard electronically held data). Reasonableness turns on the amount and sensitivity of the information the company handles (going to the magnitude of injury

from unauthorized access to information) and the nature and scope of the firm's activities (going to the structure of the firm's network, how the network operates, the types and severity of security vulnerabilities, threats, and risks it faces, and feasible protections).

II. COMPLAINT COUNSEL HAS PROVEN RESPONDENT'S DATA SECURITY PRACTICES WERE UNREASONABLE AND LIKELY TO CAUSE SUBSTANTIAL INJURY TO CONSUMERS

A. Respondent Failed to Provide Reasonable Security

Complaint Counsel presented ample evidence to show that LabMD failed to provide reasonable security for the sensitive consumer information that it maintains. Complaint Counsel showed that: (1) LabMD failed to develop, implement, or maintain a comprehensive information security program to protect consumers' Personal Information;[4] (2) LabMD failed to use mechanisms sufficient to identify or assess risks and vulnerabilities to the Personal Information maintains on its computer network;[5] (3) LabMD cannot specify the types of Personal

---

[4] CX0733 (Boyle Invest. Hrg. Tr.) at 78-79, 91-92 (stating that prior to 2010 LabMD had no written security policies). The only document that existed that related to information security was an employee handbook, which identified confidentiality as a general security goal. CX0001 (LabMD Employee Handbook Rev. June 2004) at 5-6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6 (both stating that LabMD takes "specific measures" to protect personal information from sharing and indicating that employees will "learn more," but providing no additional information). The handbook did not explain what, if any, mechanisms LabMD implemented to achieve the goal, and no LabMD employee could describe what mechanisms LabMD implemented to achieve the stated compliance goal. CX0725 (Martin Dep. Tr.) at 166-67; CX0711 (Dooley Dep. Tr.) at 144-45; CX0719 (Hyer Dep. Tr.) at 162-63; CX0733 (Boyle Invest. Hrg. Tr.) at 248-49; CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 119 (stating that employee handbook not specific on security measures); 135-37 (cannot identify documentation of measures taken to comply with HIPAA).

[5] CX0035 (Automated PC Technologies, Inc. ("APT") Service Invoice) at 2 (indicating that antivirus software on critical servers was not scanning for viruses); CX0731 (Truett Dep. Tr.) at 67-69 (stating that firewall had no monitoring features and that firewall logs were reviewed only on an ad hoc basis); CX0735 (Kaloustian Invest. Hrg. Tr.) at 177-78 (stating that manual inspection of computers was not done on a regular basis); CX0734 (Simmons Invest. Hrg. Tr.) at 78-80, 85-86 (stating that manual inspection of computers was not done on a regular basis); CX0707 (Bureau Dep. Tr.) at 50-52 (stating that manual inspection of computers were not

Information that each of its employees was permitted to access via LabMD's network,[6] and LabMD allowed employees to have access to information they did not need to perform their jobs by, among other things, maintaining the Personal Information of consumers for whom it did no testing;[7] (4) LabMD did not adequately train its employees to safeguard Personal Information;[8] (5) LabMD did not require employees or other users with access to its network to use common,

---

conducted on a regular basis); CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 150-52 (penetration tests were first performed in May 2010); CX0735 (Kaloustian Invest. Hrg. Tr.) at 92, 282 (stating that no penetration tests were performed during his time at LabMD); CX0719 (Hyer Dep. Tr.) at 164, 175-76 (LabMD did not run its own internal penetration tests before the May 2010 Providyn scans were done); CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 5 (authorizing performance of network testing on May 18, 2010).

[6] CX0754 (LabMD's Supp. Resp. to First Set of Complaint Counsel's Interrogs. to Resp't) Interrog. 2.

[7] JX0001 (Joint Stipulations of Fact, Law, and Authenticity) Stip. of Fact ¶ 5; CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 23 (admitting that LabMD maintains information on its network about more than 750,000 consumers); CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 185-90, 192-94, 198-99 (LabMD performed no tests for 20-25% of consumers on whom it received and maintains Personal Information, and other labs performed tests on 20-25% of patients for whom LabMD did not perform tests). Based on these data, LabMD maintains the Personal Information of no fewer than 100,000 consumers for whom it performed no lab test. *See also* CX0718 (Hudson Dep. Tr.) at 23-24; 52-54, 59-62 (testifying that, beginning in January 2005, it was LabMD's practice to transfer every patient's information to the company, regardless of whether LabMD performed a test for the patient); CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 43-45, 80 (testifying that the name, date of birth, address, Social Security number, billing and insurance information of all Southeast Urology Network patients was sent to LabMD, regardless of whether LabMD performed tests for the patients).

[8] CX0734 (Simmons Invest. Hrg. Tr.) at 52-53, 60-61 (stating that IT personnel did not receive IT training); CX0735 (Kaloustian Invest. Hrg. Tr.) at 208-09 (stating that IT personnel did not receive IT training). *See also* CX0705 (Bradley Dep. Tr.) at 145-47; CX0706 (Brown Dep. Tr.) at 90-93; CX0711 (Dooley Dep. Tr.) at 148; CX0714 (Former LabMD Employee Dep. Tr.) at 85-87; 96-97; CX0718 (Hudson Dep. Tr.) at 52-54, 73; CX0719 (Hyer Dep. Tr.) at 160-62; CX0724 (Maire Dep. Tr.) at 32; CX0734 (Simmons Invest. Hrg. Tr.) at 61-62; CX0735 (Kaloustian Invest. Hrg. Tr.) at 128-30, 214-15 (LabMD did not provide its non-IT employees with any training regarding security mechanisms or the consequences of reconfiguring security settings in applications).

effective authentication-related security measures, such as strong passwords;[9] (6) LabMD failed to adequately maintain and update operating systems of computers and other devices on its network;[10] and (7) LabMD failed to employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network.[11] The evidence presented

[9] CX0706 (Brown Dep. Tr.) at 13 (stating that she used the same easily guessable username and password for over six years); CX0719 (Hyer Dep. Tr.) at 26-27, 83-84 (stating that as late as 2009, LabMD did not have a strong password policy and that employees were sharing logins); CX0735 (Kaloustian Invest. Hrg. Tr.) at 79 (stating that administrative passwords were given out freely to employees).

[10] CX0070 (Providyn Network Security Scan – Mapper) (scan showing that several known vulnerabilities were found on LabMD's computers years after the vulnerabilities had been identified to IT practitioners); CX0035 (Invoice showing that software updates had not been applied); LabMD's servers were running the Windows NT 4.0 operating system in 2006, CX0735 (Kaloustian Invest. Hrg. Tr.) at 271-74, two years after Microsoft recommended that customers migrate their servers to "'more secure Microsoft operating system products as soon as possible.'" CX0740 (Expert Report of Raquel Hill, Ph.D.) ¶ 100.

[11] CX0735 (Kaloustian Invest. Hrg. Tr.) at 98-103 (stating that firewalls were not set up to block incoming network connections). *See also* CX0730 (Simmons Dep. Tr.) at 24-25, 54-56 (LimeWire installed on billing manager's computer in 2005 or 2006; LabMD did not use tools that could have detected the installation or use of a P2P application); CX0735 (Kaloustian Invest. Hrg. Tr.) at 269-70 (LabMD did not use tools that could have prevented or detected the installation or use of a P2P application); CX0711 (Dooley Dep. Tr.) at 117-19 (LabMD did not effectively prohibit or have the capability to detect the installation of a file-sharing application).

shows that LabMD's data security fell well below the standard of reasonableness,[12] with multiple failures that could have been remedied at little or no cost.[13]

B. Respondent's Security Failures Caused or are Likely to Cause Substantial Injury to Consumers

Respondent argues that Complaint Counsel has failed to make a *prima facie* case because it has not satisfied the injury element of the Section 5 unfairness standard. In support of this argument, Respondent contends that Complaint Counsel has failed to establish a causal connection between its data security practices and the exposure of the 1718 File and the Day Sheets or name specific victims. Mot. to Dismiss at 1, 3. Respondent's argument is without merit.

The first part of Respondent's argument misconstrues both the basis of this case and the testimony of Complaint Counsel's experts.[14] Respondent focuses on two incidents in which

---

[12] CX0740 (Expert Report of Raquel Hill) ¶ ¶ 49, 107; Hill, Trial Tr. May 20, 2014 at 85, 124, 203; *see also* CX0740 (Expert Report of Raquel Hill) ¶ 61 (concluding that LabMD did not develop, implement or maintain a comprehensive security program), ¶¶ 68-77 (concluding that LabMD did not employ adequate risk assessment measures), ¶ 84 (concluding that LabMD did not use adequare measures to prevent employees from accessing personal information that was not needed to perform their jobs), ¶¶ 90-91 (concluding that LabMD did not provide adequate training to IT and non-IT employees), ¶ 95 (concluding that LabMD did not use common, effective authentication-related security measures), ¶ 100 (concluding that LabMD did not adequately maintain and update operating systems of computers and other devices on its network), ¶ 105 (concluding that LabMD did not employ readily available measures to prevent or detect unauthorized access to personal information on its network).

[13] Hill, Trial Tr. May 20, 2014 at 124 (LabMD could have corrected its security failures at low cost), 132 (LabMD could have developed a comprehensive security plan at a low cost), 136 (LabMD could have developed a process-based approach to security for only cost of time spent by its IT staff), 161-62 (risk assessment tools could be obtained at low cost), 166 (employee access to information could be limited at low cost), 173-74 (training could be developed at low cost), 194 (LabMD could update operating systems and applications at no cost), 202 (employees could have been denied administrative access to their computers at no cost); *see also* CX0740 (Expert Report of Raquel Hill, Ph.D.) at ¶¶ 60; 62; 71; 77; 80(b); 85; 89; 92; 95-96; 100(d)-(e); 101; 104(a), (b), (d), (f), (h); 106.

sensitive Personal Information it maintains was improperly exposed and states that one could "conclude" that these instances could have occurred even if it had employed the security procedures that were consistent with those recommended by Dr. Hill. Mot. to Dismiss at 5-6. This contention misses the mark because it is counterfactual. Complaint Counsel has challenged Respondent's systemic failure to reasonably protect the sensitive Personal Information it maintains. Complaint Counsel has put forth ample evidence, including statements by LabMD's IT staff,[15] third-party scans of LabMD's network, and expert testimony, detailing the ways in which Respondent's security program was unreasonable. Complaint Counsel has also shown that this unreasonable security is likely to harm consumers by exposing sensitive Personal Information to an increased risk of breach or other improper disclosure.[16]

---

[14] Respondent argues that Complaint Counsel's experts' testimony should be stricken. Mot. to Dismiss at 6-7 n.6. Yet again Respondent seeks what has previously been denied on several occasions. The Court has repeatedly denied Respondent's *Daubert* motions, both in motions practice and from the bench and should do so again.

[15] Respondent suggests that Mr. Kaloustian's testimony was taken improperly. Mot. to Dismiss at 2 n.2. In its September 24, 2013 Initial Disclosures, in addition to identifying Mr. Kaloustian as a person with information relevant to its complaint, Complaint Counsel provided the transcript of Mr. Kaloustian's investigational hearing and all its attendant documents. The investigational hearing transcript and materials were produced on September 24, 2013 as FTC-000513 through FTC-000656. Respondent was informed of the investigational hearing well before the close of discovery and the Court's deadline for filing motions *in limine*. Respondent has not previously filed a motion *in limine* to exclude the testimony, and in fact stipulated to the admission of the transcript of Mr. Kaloustian's Investigational Hearing. JX002 at 18. In any event, the Commission's Rules allow for the admission into evidence of transcripts of investigational hearings. Rule 3.43(b), (e).

[16] *See* CX0067 (Providyn Network Security Scan - LabNet) at 8 (showing an "Urgent Risk" created by use of a default administrative password for backup software on a LabMD server used to maintain sensitive information); CX0070 (Providyn Network Security Scan – Mapper) at 5-7 (showing an "Urgent Risk" created by anonymous FTP on a LabMD server used to receive sensitive Personal Information from physicians' offices); CX0740 (Expert Report of Raquel Hill, Ph.D.) ¶ 31(a) (maintaining sensitive information that is not needed creates an unnecessary risk), ¶ 44 (P2P software creates risk of inadvertently sharing sensitive information in a manner that is difficult to undo), ¶ 76 (use of anonymous FTP created an "urgent risk to an application that LabMD used to transmit large amounts of Personal Information."), ¶ 79 (keeping more

The fact that Complaint Counsel can point to specific instances of data exposure – including the release of the 1718 File and the Day Sheets – strengthens, rather than undermines, Complaint Counsel's position. Moreover, while not required to prove its case in chief, Complaint Counsel has presented evidence supporting a finding that the release of information was likely the result of Respondent's overall inadequate data security practices. For instance, Complaint Counsel has presented evidence that LimeWire was installed on a computer used by the billing manager[17] and was sharing the 1718 File on the Gnutella peer-to-peer network,[18] and that LabMD had failed to take reasonable measures to prevent the installation of LimeWire or its

---

information than was needed increased the scope of potential harm), ¶¶ 81-82 (failure to limit access to data increases the likelihood that sensitive data will be "exposed . . . by either a malicious insider or a compromised system."), ¶¶ 98-99 (software should be updated to remediate bugs which can be used "to gain unauthorized access to computer resources and data."), ¶ 100(d) (LabMD's use of default administrative password on Veritas Backup software could enable attackers to "compromise the entire host")**;** Tr. of Rick Kam Testimony May 22, 2014 at 463-64 (opining that LabMD's failure to provide reasonable security increased the risk of unauthorized disclosure of the information it maintains.); CX0742 (Export Report of Rick Kam) at 23 (LabMD's failure to provide reasonable security for sensitive information it maintains created "an elevated risk of unauthorized disclosure of this information."); CX0741 (Expert Report of James Van Dyke) at 3, 6 (reaching opinion that LabMD's unreasonable security placed consumers at significantly higher risk of becoming victims of identity theft); *see also* CX0740 at 8-9 (stating that defense in depth reduces likelihood that an attack will succeed); Van Dyke, Trial Tr. May 22, 2014 at 589 (stating that there is a correlation between exposure of consumer information and identity theft); CX0741 (Export Report of James Van Dyke) at 8 (demonstrating correlation between data breaches and identity theft).

[17] *See* JX0001 (Joint Stipulations of Fact, Law, and Authenticity) Stip. of Fact ¶ 10; CX0155 (Screenshot: Start Menu: LimeWire) (showing LimeWire installed on billing manager's computer); CX0730 (Simmons Dep. Tr.) at 42-43 (stating that LimeWire was installed on billing manager's computer).

[18] *See* JX0001 (Joint Stipulations of Fact, Law, and Authenticity) Stip. of Fact ¶ 11; CX0152 (Screenshot: LimeWire: My Shared Files) (showing 1718 file in the LimeWire shared folder on billing manager's computer); CX0730 (Simmons Dep. Tr.) at 36-39 (stating that the insurance aging file was found in the LimeWire shared folder on billing manager's computer).

use to share files.[19] As a result, this file was subsequently found on four different locations on the Gnutella network, from which it could be re-shared.[20] The discovery of the Day Sheets in the hands of individuals who pleaded no contest to identity theft likewise illustrates the dangers posed by LabMD's unauthorized disclosure of Personal Information.

Respondent's position that Complaint Counsel must identify particular consumers who have already suffered identity theft, medical theft, or other type of fraud due to its unreasonable data security practices also fails. Respondent's framing of Complaint Counsel's burden of proof, "a preponderance of the evidence [of] a consumer injury that is substantial, tangible, and more than merely speculative," Mot. to Dismiss at 6, is incorrect as a matter of law. Section 5(n) of the FTC Act expressly states that an act or practice may be unfair where it "causes ***or is likely to cause*** substantial injury to consumers …." 15 U.S.C. § 45(n) (emphasis added). Thus, on its face, Section 5 recognizes that Complaint Counsel does not need to wait for harm to manifest before challenging conduct that is likely to cause consumer injury.

---

[19] *See* CX0734 (Simmons Invest. Hrg. Tr.) at 78-80 (stating that IT staff did not conduct manual inspections of computers on a regular basis, but only in response to user complaints); CX0707 (Bureau Dep. Tr.) at 50-52 (stating that manual inspection of computers were not conducted on a regular basis); CX0730 (Simmons Dep. Tr.) at 24-25, 54-56 (LimeWire installed on billing manager's computer in 2005 or 2006; LabMD did not use tools that could have detected the installation of a P2P application); CX0735 (Kaloustian Invest. Hrg. Tr.) at 269-70 (LabMD did not use tools that could have prevented or detected the installation of a P2P application); CX0711 (Dooley Dep. Tr.) at 117-19 (LabMD did not effectively prohibit or have the capability to detect the installation of a file-sharing application); CX0740 (Expert Report of Raquel Hill, Ph.D.) ¶ 68(c) (stating that manual inspections are inadequate to detect unauthorized software, even when done on a regular basis), ¶ 104(a) (stating that LabMD could have prevented the installation of LimeWire by employees at zero cost by giving employees non-administrative accounts on workstations), ¶ 105(f) (concluding that LabMD did not employ readily available measures to prevent or detect the installation of LimeWire on the billing manager's computer);

[20] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 50-51 (stating that 1718 file was located at four different IP addresses).

"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." Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) (Unfairness Statement) at 5, n.12 (*reprinted in In re Int'l Harvester Co*., 104 F.T.C. 1070, 1073 (Dec. 21, 1984)). Courts have recognized that Section 5 applies where there is the likelihood of such substantial consumer injury. S*ee FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157-58 (9th Cir. 2010) ("An act or practice can cause 'substantial injury' by doing a 'small harm to a large number or people, or if it raises a significant risk of concrete harm.'") (quoting *Am. Fin. Svcs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985) *cert. denied*, 475 U.S. 1011 (1986); *cf. In re Int'l Harvester Co.*, 104 F.T.C. 949, n. 45 (noting that while not usual, the reference to "risk" in the Unfairness Statement's discussion of an unfairness case involving health and safety risks "makes clear [that] unfairness cases may also be brought on the basis of likely rather than actual injury"); *FTC v. Accusearch, Inc.*, No. 06-CV-105-D, 2007 WL 4356786, at *8 (D.Wyo. Sept. 28, 2007) (sale of consumers' confidential phone records to stalkers and abusers was unfair because it "constitutes a clear and unwarranted risk to those consumers' health and safety"), *aff'd* 570 F.3d 1187 (2009); Statement of Basis and Purpose, Debt Settlement Amendments to Telemarketing Sales Rule, 75 Fed. Reg. 48458, 48482, n.334 (Aug. 10, 2010) (stating that while in rulemaking proceeding there was evidence that the collection of advance fees causes actual harm, the Section 5 unfairness standard does not require the Commission to "demonstrate *actual* consumer injury, but only the *likelihood* of substantial injury) (emphasis in the original).[21]

---

[21] Respondent also attempts to conflate Article III standing with the unfairness standard of the FTC Act, citing courts' decisions that an increased risk of identity theft to consumer victims of data breaches does not constitute injury for purposes of standing. *See* Mot. to Dismiss at 7 (citing, *e.g., In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 2014 U.S.

Respondent's argument relies on both a misreading of the injury component of the Section 5 unfairness standard as well as a faulty underlying assumption – *i.e.*, that Respondent's unreasonable data security practices have not injured consumers. *See supra* nn.18-21 and accompanying text. Indeed, Respondent maintains the types of sensitive Personal Information related to consumers' health – including diagnoses, test results, test codes, and health insurance company names and policy numbers[22] – that, if exposed, can lead to medical identity theft, which can cause substantial consumer injury in the form of financial, reputational, and other harms.[23] Similarly, the release of Social Security numbers, bank account and credit information, and other

---

Dist. Lexis 64125 (D.D.C. May 9, 2014); *but see id.* at *35-36 (disclosure of personally identifiable information alone in violation of a consumer's privacy, along with attendant emotional injury, may constitute injury for standing purposes)). However, the standing analysis applied by the courts Respondent cites is inapposite; a private plaintiff must demonstrate an "injury in fact" for Article III standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

Section 5 of the FTC Act does not require injury in fact. *Lujan*'s injury-in-fact element stands in stark contrast to Section 5's "likely to cause substantial harm" standard. *See, e.g.*, *Am. Fin. Svcs. Ass'n v. FTC*, 767 F.2d 957, 973-74 (D.C. Cir. 1985) (determining that Commission's findings that, *inter alia*, security interest in household goods can make consumers desperate and amenable to future suggestions of unfavorable transactions satisfied Section 5 unfairness injury requirement); *In re Philip Morris, Inc.*, 82 F.T.C. 16 (Jan. 9, 1973) (finding that although there was no evidence of past injury, distribution of razor blades in newspapers likely to cause injury to newspaper carriers, children, and pets and declaring the practice unfair). Furthermore, Respondent ignores the courts that have reached the opposite conclusion in analyzing injury from data breaches for standing purposes. *See, e.g.*, *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (theft of laptop containing person data created "credible threat of real and immediate harm" of future identity theft); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (threat of future harm from identity theft satisfies injury-in-fact requirement).

[22] *See* JX0002 (Joint Stipulations of Law, Fact, and Admissibility) Stip. of Fact ¶ 4.

[23] Kam, Trial Tr. May 21, 2014 at 395-96; *see also* Kam, Trial Tr. May 22, 2014 at 445-53 (exposure of 1718 file was likely to lead to reputational harm to consumers based on the release of sensitive information about medical tests performed on consumers); CX0742 (Expert Report of Rick Kam) at 16, 21 (victims who may have cancer or sexually transmitted diseases are particularly vulnerable to reputational harm); CX0741 (Expert Report of James Van Dyke) at 13 (medical identity theft can lead to financial harm as well as direct physical harm).

Personal Information can result in identify theft and other forms of fraud.[24] It may take consumers years to discover that thieves have stolen their identities.[25] As Complaint Counsel's experts have testified, it may be difficult for consumers to determine that their Personal Information has been misused by identity thieves.[26] Even when consumers realize that they have been victimized, in cases such as this one where none of the consumers in that 1718 File were notified that their Personal Information had been exposed, it can be difficult for them to connect the identity theft to the company responsible for the exposure.[27] Accordingly, Respondent incorrectly presumes that its unreasonable data security practices have not already subjected consumers to identity theft.

Complaint Counsel also has put forth evidence regarding the severity of the harm that identity theft and medical identity theft can inflict on consumers. This includes financial harm, reputational harm, and time spent repairing those harms.[28] In cases of medical identity theft, the

---

[24] CX0742 (Expert Report of Rick Kam) at 10-11; Kam, Trial Tr. May 22, 2014 at 475 (Social Security numbers and consumer name can be used to commit identity theft); *see also* Kam, Trial Tr. May 21, 2014, at 412-13 (testifying the Social Security numbers are sold on the black market by identity thieves); Kam, Trial Tr. May 22, 2014 at 476-77 (testifying that Social Security numbers and checking account numbers can be used for account takeover); CX0741 (Expert Report of James Van Dyke) at 5 (name, address, and Social Security numbers can "be leveraged by fraudsters for an extended period of time.").

[25] CX0742 (Expert Report of Rick Kam) at 12; Kam, Trial Tr. May 22, 2014, at 479 (Social Security numbers can be used by identity thieves years after they are stolen).

[26] Kam, Trial Tr. May 21, 2014, at 396; CX0742 (Expert Report of Rick Kam) at 12

[27] Kam, Trial Tr. May 21, 2014, at 398; Kam, Trial Tr. May 22, 2014, at 466; CX0742 (Expert Report of Rick Kam) at 17 (stating that, absent breach notification, "consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information.").

[28] Kam, Trial Tr. May 21, 2014 at 394-95; CX0742 (Expert Report of Rick Kam) at 14-15; CX0741 (Expert Report of James Van Dyke) at 9 (stating that victims of identity theft suffer significant financial costs, with victims of new account fraud losing an average of $449), 9-10 (stating that identity theft victims spend significant amount of time resolving problems caused by the crimes, with new account fraud victims spending an average of 26 hours), 12 (projecting total

risk of harm is even more severe, as consumers are exposed to the risk of misdiagnosis, improper or delayed treatment, having the wrong pharmaceuticals prescribed, and loss of insurance.[29] As noted above, even small amounts of injury to large numbers of consumers constitute substantial injury for purposes of unfairness under Section 5. Here, given the large number of consumers whose Personal Information Respondent failed to adequately secure, coupled with the potential economic, health and safety, and other well documented consumer harm caused by identity and medical identity theft, it is clear that the risk of injury is profound.

---

consumer losses of over $35,000 and over 2,497 resolution hours spent as a result of identity theft caused by the exposure of LabMD's day sheets); Van Dyke, Trial Tr. May 22, 2014 at 595 (stating that identity theft victims must spend significant time to resolve the effects of these crimes); 597-98 (stating that identity theft causes significant losses to businesses, organizations, and consumers).

[29] Kam, Trial Tr. May 21-22, 2014, at 427-430, 441-43; CX0742 (Expert Report of Rick Kam) at 15-16, 20-22.

CONCLUSION

For the foregoing reasons, Respondent's Motion to Dismiss should be denied. Respondent misconstrues the law of unfairness, and Complaint Counsel has met its burden of proof that Respondent's conduct was likely to cause consumers substantial harm.

Dated: June 6, 2014

Respectfully submitted,

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown

Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-2999 – VanDruff
Facsimile: (202) 326-3062
Electronic mail: lvandruff@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on June 6, 2014, I filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

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

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

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

Michael Pepson
Lorinda Harris
Hallee Morgan
Robyn Burrows
Kent Huntington
Daniel Epstein
Patrick Massari
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
michael.pepson@causeofaction.org
lorinda.harris@causeofaction.org
hallee.morgan@causeofaction.org
robyn.burrows@causeofaction.org
kent.huntington@causeofaction.org
daniel.epstein@causeofaction.org
patrick.massari@causeofaction.org

Reed Rubinstein
William A. Sherman, II
Sunni Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004

reed.rubinstein@dinsmore.com
william.sherman@dinsmore.com
sunni.harris@dinsmore.com
Counsel for Respondent LabMD, Inc.

CERTIFICATE FOR ELECTRONIC FILING

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

June 6, 2014 By: Megan Cox

Megan Cox
Federal Trade Commission
Bureau of Consumer Protection