PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of

LabMD, Inc.,
a corporation.

DOCKET NO. 9357

PUBLIC

ORAL ARGUMENT REQUESTED

RESPONDENT LabMD, INC.'S MOTION FOR SUMMARY DECISION

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9100
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

TABLE OF CONTENTS

RESPONDENT LabMD, INC'S MOTION FOR SUMMARY DECISION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

Please take notice that, pursuant to Commissions Rules 3.22 and 3.24, 16 C.F.R. §§ 3.22 and 3.24, Respondent LabMD, Inc., hereby moves for summary decision in its favor, and requests that the Administrative Complaint be dismissed in its entirety with prejudice.

INTRODUCTION

LabMD, Inc. ("LabMD") is being singled out by the Federal Trade Commission ("FTC") for its allegedly deficient data-security practices. All information received, utilized, maintained and transmitted by LabMD is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *See* 45 C.F.R. § 160.103. The FTC takes the position that it has Section 5 unfairness authority to create and enforce opaque "common law" regulations governing PHI data-security. Currently, the FTC's opaque "common law" regulations consist of negotiations, consent decrees, public statements made by the Commission, educational materials and internet posts which when taken together create additional and far more stringent and inconsistent standards than those promulgated by the Department of Health and Human Services ("HHS").[1] Even if FTC has such authority, it has failed to provide the constitutionally required fair notice of the PHI data-security standards that it seeks to enforce.

After more than four years of thorough investigation and litigation, including the depositions of FTC's Rule 3.33 designee and expert witnesses, FTC continues to take the position that it is not constitutionally required to specify in advance of investigation and

[1] HHS was granted Congressional rulemaking authority and promulgated regulations governing PHI data security standards through transparent, public notice and comment rulemaking.

litigation the FTC data-security standards applicable to LabMD or similarly situated HIPAA "Covered Entities." *See* 45 C.F.R. § 160.103.

STATEMENT OF FACTS

The following facts are undisputed:

LabMD is a small, privately-owned medical laboratory providing cancer diagnoses through blood, urine, and tissue sample testing. Its customers are physicians. The physicians send their samples to LabMD, together with the relevant patient identification and insurance information, and LabMD sends back to the physicians the relevant diagnosis.

LabMD is a "Covered Entity" that receives, maintains and transmits PHI during the normal course of its business. *See* 45 C.F.R. § 160.103.

On or about February 5, 2008, without LabMD's knowledge or consent, Tiversa, Inc. ("Tiversa"), took possession of a single LabMD insurance aging file (the "Insurance Aging File"). Deposition of Robert Boback, dated Nov. 21, 2013, at 25, attached hereto as Exh. 1.[2]

The Insurance Aging File contained PHI for over 9,000 patients of LabMD's physician clients.

Subsequently, Tiversa made the Insurance Aging File available to Professor Eric Johnson, of Dartmouth College, who was conducting research under a government contract for his article entitled, "Data Hemorrhages in the Health Care Sector". *See* Data Hemorrhages in the Health-Care Sector at 1 fn. 1, attached in relevant part hereto as Exh. 2.

In January 2010, the FTC began a three year full investigation of LabMD's data security practices based upon the disclosure of the PHI contained in the Insurance Aging File.

[2] Tiversa has testified before Congress that it possesses unique technology which among other things allows it to download computer files from unsuspecting third persons inadvertently sharing computer files via peer to peer ("P2P") networks. *See Hearing Before the H. Subcomm. on Commerce, Trade, & Consumer Protection*, 111th Cong. 3-4 (2009)(statement of Robert Boback, CEO, Tiversa, Inc.).

In October 2012, during a raid of a house of suspected identity thieves, the Sacramento Police Department found LabMD "day sheets" and copies of checks made payable to LabMD. Again, the day sheets and checks contained PHI from patients of LabMD's physician clients. Deposition of Detective Jestes, dated Dec. 17, 2013, at 29-30, 33-36, attached hereto as Exh. 3.

In an attempt to notify LabMD of its find, the Sacramento police "googled" LabMD, and discovered that LabMD was under investigation by the FTC. Deposition of Detective Jestes, dated Dec. 17, 2013, at 27-28, 56, attached hereto as Exh. 3.

The Sacramento police then notified the FTC of its find, but did not notify LabMD, despite Sacramento's awareness of LabMD's duty to notify under HIPAA. Deposition of Detective Jestes, dated Dec. 17, 2013, at 28, attached hereto as Exh. 3.

In August, 2013, FTC filed an Administrative Complaint. *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("Compl.") (Aug. 28, 2013).

LabMD is a HIPAA-covered entity. Opp'n to Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD Opp'n") (Nov. 22, 2013) at 22 fn 15. It must comply with HHS's HIPAA and Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations, including HHS's HIPAA Privacy Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000); HHS's HIPAA Security Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003); and HHS's HITECH Breach Notification Rule, 78 Fed. Reg. 5,566 (Jan. 25, 2013).

HIPAA's Security Rule establishes substantive data-security standards involving PHI with which HIPAA-covered entities, like LabMD, must comply.

HHS exclusively enforces HIPAA and HITECH. Order on Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD Order")(Jan. 16, 2014), at 12 & n.19

("[T]he Commission cannot enforce HIPAA and does not seek to do so. ... The Commission does not enforce HIPAA or HITECH....").

The FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations. Compl. ¶¶ 22-23; Initial Pretrial Conference Transcript, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, 22:10-13 (Sept. 25, 2013) ("Trans."); MTD Order at 12 n. 20 (Jan. 16, 2014); Complaint Counsel's Resp. to LabMD's RFAs, ("CC's RFA Responses") at 8-9 ¶¶ 7-8, attached hereto as Exh. 4.

The FTC alleges that LabMD's data-security is inadequate to protect the PHI it possesses and that this failure to adequately protect PHI is an unfair practice affecting consumers in violation of Section 5 of the Federal Trade Commission Act.

The FTC's expert opines that these failures persisted from January 2005 through July 2010 ("the relevant time period"). *See* Complaint Counsel's Expert Report of Professor Raquel Hill at 1, attached hereto as Exh. 5.

The FTC has never specified what data security standards were in place at any given point during the relevant time period or when LabMD specifically violated them.

The FTC claims it need not "allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use." CC's RFA Responses at 6-7 ¶ 5, attached hereto as Exh. 4.

When asked by the ALJ whether "the Commission issued guidelines for companies to utilize to protect...[sensitive] information or is there something out there for a company to look to," the FTC admitted that "[t]here is nothing out there for a company to look to." Trans. 9:13-18.

The FTC admits that it has never promulgated data-security regulations, guidance, or standards under Section 5: "[T]here is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act...for financial institutions." Trans. 10:11-15.

When asked about other sources of data-security standards, FTC said: the "Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness." Trans. 9:18-22. The FTC also stated that "public statements made by the Commission" and so-called "educational materials" were standards. *Trans.* 9:23-25. And finally the FTC argued that "the IT industry...has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology that the Commission is following in deciding reasonableness," except that the "Commission's process" involves "calculation of the potential consumer harm from unauthorized disclosure of information." Trans. 10:1-7.

In response to LabMD's written discovery requesting documents relating to the standards the FTC enforces regarding data-security, the FTC produced thousands of pages of consent decrees, reports, PowerPoint presentations, and articles from the FTC's website, including many in Spanish. Ltr. from L. VanDruff, dated Jan. 27, 2014, attached hereto as Exh. 6 (showing that the FTC produced thousands of documents responsive to Request 10, which requested documents pertaining to the standards the FTC enforces); Ltr. from L. VanDruff, dated Mar. 3, 2014, attached hereto as Exh. 7 (same); Example of Production, attached hereto as Exh. 8.

At the hearing, the ALJ asked: "Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?" The FTC responded "No." Trans. 22:10-13.

The FTC also admits that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Trans. 20:15-17.

STANDARD OF REVIEW

Commission Rule 3.24 provides that "[a]ny party ... may move ... for a summary decision in the party's favor upon all or any part of the issues being adjudicated." 16 C.F.R. § 3.24(a)(1). Rule 3.24 further provides that if the Commission determines that there is no genuine issue as to any material fact regarding liability or relief, it shall issue a final decision and order. 16 C.F.R. § 3.24(a)(2).

When a motion for summary decision is made and adequately supported, "a party opposing the motion may not rest upon the mere allegations or denials of his or her pleading; the response, by affidavits or as otherwise provided in this rule, must set forth specific facts showing that there is a genuine issue of material fact for trial." 16 C.F.R. §3.24(a)(3). Once the moving party has adequately supported its motion, the nonmoving party must "do more than simply show that there is some metaphysical doubt as to the material facts." *In re North Carolina State Board of Dental Examiners*, 151 F.T.C. 607, 611 (2011) (internal citations and quotation marks omitted). The non-moving party must instead establish "specific facts showing that there is a genuine issue for trial." *Id.* (internal citations and quotation marks omitted); *see also* 16 C.F.R. § 3.24(a)(3). And "[w]here the record taken as a whole could not lead a rational trier of fact to find for the nonmoving party, there is no 'genuine issue for trial.'" *North Carolina*, 151 F.T.C. at 611 (internal citations and quotation marks omitted).

ARGUMENT

I. SECTION 5's UNFAIRNESS PROVISION DOES NOT AUTHORIZE FTC TO CREATE A COMMON LAW OF PHI DATA SECURITY.

LabMD believes that FTC lacks Section 5 "unfairness" authority to regulate data-security generally, and specifically for PHI. *See* Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD") (Nov. 12, 2013); Reply to Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("Reply to MTD") (Dec. 2, 2013). For the reasons set forth therein, the Commission's MTD Order is wrongly decided and summary decision for LabMD should be granted.[3]

The PHI in LabMD's possession is information that patients voluntarily gave to their doctors, who in turn, voluntarily provided this information to LabMD. Even so, the Commission claims that Section 5's unfairness authority sanctions the use of legal process against LabMD "to protect consumers from unwanted privacy intrusions..." MTD Order at 1. This claim, however, conflicts with the United States government's long-standing assertion that consumers who voluntarily provide personal information to third parties lose their privacy rights because the information in question, once given, belongs to the receiver and not the consumer. *See, e.g.*,

[3] Worldwide Corporation, Order on Mot. to Dismiss No. 2:13-CV-01887-ES-JAD, Dkt. 181,(D. N.J., Apr. 7, 2014)("Wyndham Order on Mot. to Dismiss") is not a PHI case. But it too is wrongly decided. Using a tautology - FTC has sweeping authority because it has sweeping authority - the court dodged the hard legal question: Does FTC's roughly fifty consent orders and internet posts constitute adequate fair notice? The district court noted the "rapidly-evolving nature of data security" and quoted *General Electric v. Gilbert*, 429 U.S. 125 (1976) for the proposition that "the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance." Wyndham Order on Mot. to Dismiss at 24. However, the court omitted the very next sentence: "The weight of such a judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control." *See Gilbert*, 429 U.S. at 142 (citation omitted).

The Wyndham court noted that Congress has prescribed a three-part standard for unfairness but fail utterly to assess whether FTC has thoroughly or rigorously applied that standard, or whether the approach it has taken is really an end run of Congressional efforts to prevent unelected bureaucrats from avoiding accountability and transparency. The idea that FTC has the unbounded power to create a law of data security, binding on all companies economy-wide using nothing more than ad hoc consent orders and unilateral internet posts and without any meaningful public scrutiny or input, cannot be seriously defended. But such was the court's ruling.

Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint, *ACLU, et al., v. Clapper, et al.*, Case No. 13 Civ. 3994 (WHP), Dkt. No. 33 at 32-33 (Aug. 26, 2013)("Gov. Motion") citing *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)("a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); *United States v. Miller*, 425 U.S. 435, 440-41 (1976)(rejecting a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, inasmuch as the bank was a party to the transactions, the records belonged to the bank).[4] In other words, FTC has attacked LabMD for "misusing" its own property.

Through HIPAA, Congress created ***enforceable privacy rights*** in PHI and authorized HHS to promulgate binding regulations governing medical providers that handle it. But as FTC claims this case has nothing to do with HIPAA, MTD Order at 12 ("To be sure, the Commission cannot enforce HIPAA and does not seek to do so"), it therefore runs into a thick wall of federal arguments that conflict with FTC's foundational premise: that consumers who voluntarily give PHI to medical providers have some protectable privacy or other interest in that information beyond that which Congress authorized HHS to carve out under HIPAA. Consequently, without proof of deception, the FTC's section 5 authority does not extend to the regulating PHI. *New Hampshire v. Maine*, 542 U.S. 742, 749-50 (2001).

[4] The government argued:

> In *Smith v. Maryland*....the Court reasoned, even if a subscriber harbored a subjective expectation that the phone numbers he dialed would remain private, such an expectation of privacy would not be reasonable, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

Gov. Motion at 33 (citations omitted). Thus, "Courts have followed Smith to find no reasonable expectation of privacy in email "to/from" and Internet protocol ("IP") addressing information, in text message addressing information, and in subscriber information, such as subscribers' names, addresses, birthdates, and passwords, communicated to system operations and Internet service providers." *Id.* (citations omitted).

II. THE FTC HAS FAILED THE FAIR NOTICE TEST AND VIOLATED DUE PROCESS.

The FTC may have broad power under Section 5, but even the broadest of bureaucratic powers have constitutional limits. Due process prohibits the FTC from using legal process against LabMD without first providing fair notice, a doctrine that is "[a] fundamental principle in our legal system [requiring] that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). If a person acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects the entity to conform, the agency has not provided fair notice. *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995). Administrative law has thoroughly incorporated this constitutional fair notice requirement to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. *See Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007)("Even if the Secretary's interpretation was reasonable, announcing it for the first time in the context adjudication deprives Petitioners of fair notice); *Satellite Broadcasting Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987)(traditional concepts of due process incorporated into administrative law preclude agencies from penalizing private parties for violating rules without first providing adequate notice of their substance).

FTC has taken a variety of inconsistent positions on the matter of fair notice, ranging from "it is not obligated to provide adequate notice" to "Section 5(n) provides adequate notice." As discussed below, each of these varying positions contradicts black letter law. Here, FTC seeks to impose PHI data-security standards that conflict with HIPAA. It thereby violates LabMD's due process rights as no such separate and additional PHI data-security standards were known to exist by LabMD or any other Covered Entity.

Because the FTC has failed to provide constitutionally adequate notice to LabMD of the PHI standards it seeks to enforce, LabMD's motion for summary decision should be granted.

A. FTC Failed To Provide Constitutionally Adequate Notice Of the Data Security Standards it Currently Seeks to Impose on Entities that Possess PHI

This case is an instance in which the FTC claims the power to create its own "common law" PHI data-security requirements which are more stringent and inconsistent with those created by HHS.

For example, in *In the Matter of Rite Aid Corporation,* the FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash containing consumers' personal information such as pharmacy labels and job applications. At the same time, HHS began investigating the pharmacies' handling of PHI. *See* FTC Dkt. C-4358, http://www.ftc.gov/news-events/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-and. Eventually, FTC alleged that Rite Aid failed to protect "sensitive financial and medical information" while HHS alleged that it failed to protect PHI. *Id.* Rite Aid settled with both FTC and HHS. *Id.* FTC required Rite Aid to protect personal information while HHS's settlement required Rite Aid to protect PHI. *Id; see also In the Matter of CVS Caremark, FTC* Dkt. C-4259, http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial (involving PII and PHI data-security, where FTC used its Section 5 authority for PII and HHS used its HIPAA authority for PHI).

The FTC has taken the position that the *Rite Aid* and *CVS* cases are part of the developing common law which establishes it as having concurrent jurisdiction to enforce HIPAA. However, it is clear that those two cases involve entities that do not deal exclusively with PHI. Taken together, FTC's "common law" and the Commission's ruling in its MTD Order demonstrate that HHS has always been responsible for PHI data-security standards and that HIPAA, not Section

5's general unfairness provision, controls in this case. It is perhaps arguable through the its involvement in the *Rite Aid* and *CVS* cases, that the FTC has demonstrated that it has complementary jurisdiction to enforce PHI data-security using HIPAA standards, however the FTC has denied having such authority. Thus, there can be no dispute that the FTC's claim in this case that Section 5 authorizes it to over-regulate HIPAA and create a new law "common law" of PHI data-security is newly baked. Companies like LabMD that maintain only PHI could not have known that the FTC had decided HIPAA compliance was not enough. Simply, the FTC's prior involvement in cases such as *Rite Aid* and *CVS*, combined with its three-year investigation and creation of ex post facto "springing standards" that, by happenstance, LabMD failed to meet, is insufficient to meet LabMD's constitutional due process right to fair notice..

Instead of enforcing HIPAA standards, which provide fair notice and have been properly promulgated through notice and comment rulemaking, the FTC has now decided to hold companies like LabMD to never-before-seen and ever-changing standards that it concocts after the alleged offense has occurred. Even the FTC admits that by using its Section 5 "unfairness" authority in this manner, it is seeking to enforce standards *ex post facto*. Ohlhausen Statement at 11-13, attached as Exh. 9.

Here, FTC is seeking to enforce standards that its expert, Professor Raquel Hill, devised after reviewing three years worth of material the FTC collected during its investigation of LabMD along with testimony and materials collected during discovery. *See* Complaint Counsel's Expert Report of Professor Raquel Hill, generally, attached hereto as Exh. 5. FTC's determination to fabricate its own standards may explain why it has taken varying and inconsistent positions throughout this case.

1. The FTC is obligated to provide adequate notice of the standards it seeks to enforce.

Despite the fair notice doctrine's robust application in a variety of administrative actions, *see e.g. Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007)("Even if the Secretary's interpretation was reasonable, announcing it for the first time in the context adjudication deprives Petitioners of fair notice), the FTC has taken the position that it is not obligated to provide any fair notice at all because agencies have broad discretion to "address an issue by rulemaking or adjudication." MTD Opp'n at 15. This position was recently highlighted in the deposition of the Bureau of Consumer Protection's Rule 3.33 witness, Daniel Kaufman. Here, Respondent's counsel asked Mr. Kaufman a series of questions related to published standards that the Bureau sought to enforce against LabMD; however, Complaint Counsel instructed the witness not to respond to any of these questions. Deposition of Daniel Kaufman, Apr. 14, 2014 at 115-139, attached hereto as Exh. 10.

For example Respondent's Counsel asked Mr. Kaufman, "Based on the allegations in paragraph 10(a), my question is has the Bureau or the FTC published, and by published I mean made available to the public, the standard that it requires for a comprehensive information security program for companies like LabMD to have in place?" Complaint Counsel objected to the question stating, "I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question. . ." Deposition of Daniel Kaufman, Apr. 14, 2014 at 119, attached hereto as Exh. 10.

Complaint Counsel has taken the position that it is not required to inform LabMD of the data security standards applicable to this case despite the ALJ's March 10, 2014, Order. ("Complaint Counsel has not demonstrated that Topic 2 is entirely outside the scope of discovery, so as to bar any and all deposition testimony within its scope, and Respondent has articulated a valid line of inquiry.")

Alternatively, the FTC has argued that it is not obligated to provide fair notice because it is not seeking "criminal punishment or civil penalties for past conduct." MTD Order at 16. To the contrary, it is well settled that administrative agencies must provide fair notice not only when they pursue criminal or civil penalties, but also in cases in which they seek other kinds of burdensome relief. *See, e.g., United States v. Chrysler Corp.*, 158 F.3d 1350, 1354-55 (D.C. Cir. 1998) (holding that fair notice is required when the government seeks a product recall); *In re Bogese*, 303 F.3d 1362, 1368 (Fed. Cir. 2002)(forfeiture); *PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000) (license revocation). If the FTC is successful on the merits of its case, then LabMD will be subject to an array of burdensome financial requirements. The FTC typically reserves the right to order or seek additional relief as it sees fit, including, but not limited to permanent injunctive relief, restitution, disgorgement, rescission or reformation of contracts, payment of monetary damages, and (likely) decades of intrusive and costly external monitoring. These are "'sufficiently grave sanction[s]' such that the duty to provide notice is triggered." Chrysler, 158 F.3d at 1355.

2. *Section 5(n) does not constitute fair notice of the standards the FTC seeks to enforce against LabMD.*

FTC has argued that the plain text of Section 5(n) somehow adequately provides "a person of ordinary intelligence fair notice of what is prohibited." MTD Order at 17-18. Section 5(n) provides:

> The Commission shall have no authority under this section or section 57a of this title 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.

However, this section does no more than announce in general terms what types of consumer injuries fall within the FTC's jurisdiction. *See* 15 U.S.C. § 45(n). It does not provide any guidance whatsoever about the nature or kinds of data-security standards, methodologies, procedures, or processes a company must adopt in order to be compliant, nor does it provide even general guidance about how it measures the performance of a company's data security practices. FTC thus stretches its own credibility by arguing that the text of Section 5(n) itself somehow "provide[s] greater certainty for businesses." MTD Order at 5. Surely if the FTC believed this to be true, Professor Hill's expert analysis on whether LabMD provided "reasonable and appropriate security for Personal Information within its computer network" would have mentioned and analyzed Section 5(n). However, this opinion is devoid of any mention of Section 5(n). Complaint Counsel's Expert Report of Professor Raquel Hill, attached hereto as Exh. 5.

3. Consent Decrees, Negotiations, Public Statements made by the Commission, Reports, PowerPoint Presentations, and Articles on the FTC's website do not constitute fair notice of the standards the FTC seeks to enforce.

In LabMD's written discovery to the FTC, it requested the following documents:

> 8. All documents sufficient to show what data-security standards are currently used by the FTC to enforce the law under Section 5 of the Federal Trade Commission Act.
>
> 9. All documents sufficient to show what changes occurred in the data-security standards used by the FTC to enforce the law under Section 5 of the Federal Trade Commission Act from 2005 to present and the dates on which these standards changed.
>
> 10. All documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act form 2005 to present.

See FTC's Discovery Responses, attached in relevant part hereto as Exh. 11. In response to these discovery requests, Complaint Counsel produced thousands of pages of documents which included consent decrees, industry guidance, PowerPoint presentations, and articles on the FTC's website. *Id.*; *see also*, Ltr. from L. VanDruff, dated Jan. 27, 2014, attached hereto as Exh. 6; Ltr. from L. VanDruff, dated Mar. 3, 2014, attached hereto as Exh. 7. To the extent that Complaint Counsel wishes to assert that these materials provide adequate notice, it is incorrect.

First, the Commission cannot claim that a diffuse collection of Commission consent orders establish generally-applicable data-security standards or put the public on notice thereof. FTC cannot regulate by consent orders. *See Gen. Elec. Co. v. EPA*, 290 F.3d 377, 382-83 (D.C. Cir. 2002)(holding that agency guidance document that imposes binding duties and obligations violates the APA). Consent orders "do not establish illegal conduct," *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement." *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). Moreover, consent orders do not bind the Commission or restrict its discretion in future actions and statements that do not constrain governmental authority do not provide the fair notice that due process requires. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999). Indeed, in Section 5 itself Congress *specifically barred* the Commission from binding third parties by consent order: the Commission is statutorily prohibited from enforcing a "consent order" against anyone that is not a party to it. 15 U.S.C. § 45(m)(2); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir. 2007)("Indeed, the FTC Act...with regard to consent orders...specifically provides that the Commission cannot enforce them against non-parties.").

Moreover, general statements of policy, such as industry guidance, power point presentations, and articles on the FTC's website, are prospective and do not create obligations enforceable against third parties like LabMD. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980)("The agency cannot apply or rely upon a general statement of policy as law because a...policy statement announces the agency's tentative intentions for the future"); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006)(in holding agency manuals to be nonbinding, the court said that "it is particularly noteworthy that NPS did not issue its management policies through notice and comment rulemaking under 5 U.S.C. § 553" because failure to do so is evidence that the material in question was not supposed to be a rule binding regulated companies' conduct).

Tellingly, the FTC's expert, Professor Raquel Hill, who opined on "reasonable and appropriate security for Personal Information within its computer network" never consulted any of the materials that FTC purports it is "using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act." Complaint Counsel's Expert Report of Professor Raquel Hill at Appendix B, attached hereto as Exh. 5. Rather Ms. Hill's report consists of entirely new and never-disclosed metrics. *Id.*

III. If FTC May Over-Regulate HIPAA, It May Over-Regulate All Other Regulated Areas Affecting Consumers.

If FTC may lawfully over-regulate HHS, add to HIPAA and attack LabMD using its Section 5 unfairness authority, then, upon its determination that a given practice "is reasonably likely to cause harm to consumers," it may lawfully over-regulate drinking water governed by the Safe Drinking Water Act or food products subject to "standards of identity" established by the Food and Drug Administration such as Swiss cheese or spring water. It may over-regulate hazardous waste management practices subject to the Resource Conservation and Recovery Act and long-standing Environmental Protection Agency regulations. And, it may over-regulate in the fields of employment law or nuclear energy or any other myriad of regulated areas which naturally could harm consumers. Clearly then, there is no end to FTC's power and Section 5, most recently amended by Congress in 1994 to limit the Commission's power, is instead a gateway to total regulatory authority. Congress never intended FTC to have such sweeping and over-riding authority to intervene and superimpose new and additional requirements on entities, especially when properly promulgated regulations already exist and adequate notice has not been provided.

IV. Even If FTC Provided LabMD Fair Notice, HIPAA Controls.

In *Credit Suisse Securities (USA) LLC v. Billings*, 551 U.S. 265 (2007), the United States Supreme Court set forth the factors to consider to determine when a specific regulatory regime displaces, or implicitly precludes enforcement under, a more general and earlier enacted regulatory scheme. The Court held that the securities laws were "clearly incompatible" with the antitrust laws and therefore, held that the antitrust claims were precluded by the securities law regulatory regime. While *Credit Suisse* specifically addressed the interplay of securities regulation and antitrust law, the test and its underlying logic apply here.

The issue in *Credit Suisse* was whether a plaintiff could file antitrust claims against investment banks that had formed syndicates and engaged in other practices to form markets for initial public offerings that were actively regulated under the securities laws. 551 U.S. at 269-70. The Supreme Court applied a four-factor test to determine whether such incompatibility existed:

> [I]n finding sufficient incompatibility to warrant an implication of preclusion, have treated the following factors as critical: (1) the existence of regulatory authority under the securities law to supervise the activities in question; (2) evidence that the responsible regulatory entities exercise that authority; and (3) a resulting risk that the securities and antitrust laws, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct . . .. We also note (4) in *Gordon* and *NASD* the possible conflict affected practices that lie squarely within an area of financial market activity that the securities law seeks to regulate.

Credit Suisse, 551 U.S. at 275-76. These factors support a finding that HIPAA regulation of data security is incompatible with FTC over-regulation.

First, HIPAA directly applies and delegates rulemaking and standard setting authority to HHS. Indeed, HHS has adopted data privacy and data security rules, which it routinely enforces. *See, e.g.*, 42 U.S.C. §1320d(3)-(4) (defining terms); 45 C.F.R. § 160.103 (same); 42 U.S.C. § 1320d-2(d)(1) (establishing "Security standards for health information" and providing HHS with enforcement authority); 65 Fed. Reg. 82,462 (Dec. 28, 2000) (HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334 (Feb. 20, 2003) (HHS's HIPAA Security Rule); *see also* 78 Fed. Reg. 5,566 (Jan. 25, 2013) (HHS's HITECH Rule). These rules address the same activities that are the subject of this case.

Second, dual enforcement is resulting in (and will continue to result in) conflicting guidance and requirements. The best illustration of conflict is that LabMD's compliance with the HIPAA is not a defense to the newly created FTC regulations. Rather, FTC deems regulatory compliance to be irrelevant to, much less a defense against, Section 5 unfairness claims. *See, e.g.*, FTC's Mot. to Dismiss, *LabMD, Inc. v. Federal Trade Commission*, No. 1:14-CV-810-WSD, N.D. Georgia Dkt 18, at 27 (arguing that HHS's regulations implanting HIPAA serve to "establish a *minimum* level of security that covered entities must meet" (internal quotation omitted, emphasis in original)). This disdain creates inherent conflict and confusion among HIPAA Covered Entities

HHS's PHI data-security standards differ in material ways from the FTC's purported standards. FTC's "standards," at least as articulated by its expert, introduce additional security principles that are difficult to reconcile with Administrative, Technical and Physical main structure of the HIPAA security rule. For example, they are not scalable in accordance with the

Security Rule, [5] and do not account, as required by HIPAA, for the needs and capabilities of small health care providers and rural health care providers. [6] The recommendation for file integrity monitoring requires expertise to implement and configure these solutions and can be even more resource intensive to understand, investigate and resolve alerts from the solution.

Other FTC "standards" that are more prescriptive than HIPAA or inconsistent with HHS guidance, include encryption at rest (an addressable requirement of 164.312(a)(1)), encryption in transit (an addressable requirement of 164.312(e)(1)), intrusion detection (not addressed specifically by the Security Rule), virus protection (an addressable requirement of 164.308(a)(5)(ii)(B)), firewalls (not addressed specifically by the Security Rule), penetration testing (not addressed by the Security Rule), and file integrity monitoring (not addressed specifically by the Security Rule). The electronic health record certification requirements published for HHS for Meaningful Stage 2 in 2012 do not even require this level of encryption for all PHI stored by the system. In addition, tools such as intrusion detection and file integrity monitoring systems require experienced and committed technical resources to configure and manage.

FTC's "standards" presume a level of technical knowledge generally not available to small health care providers and conflict with HHS guidance. For example, FTC's expert almost exclusively focuses on technologies or technical processes for the risk assessment process (i.e., antivirus applications, firewalls, various types of vulnerability scans, intrusion detection systems, penetration tests, file integrity monitoring, and other measures). This is inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process.

[5] 68 Fed. Reg. 8,334, 8,335 (Feb. 20, 2003). In the preamble to the HIPAA Security Rule, HHS emphasizes that the Rule must be "scalable, so that it can be effectively implemented by covered entities of all types and sizes," and notes further that "[s]ince no comprehensive, scalable, and technology-neutral set of standards currently exists, we proposed to designate a new standard, which would define the security requirements to be fulfilled." *Id.* at 8,341.

[6] 42 U.S.C. § 1320d–2(d)(1)(A)(v).

If health care providers are going to be held to a compliance standard that is simply an expert's opinion of best practices in information security at any point in time, when that expert standard exceeds the compliance standard developed by notice and comment rulemaking under HIPAA, then the standard developed under HIPAA is made effectively meaningless, null and void. *See also* Declaration of Cliff Baker, *LabMD, Inc. v. Federal Trade Commission*, No. 1:14-CV-810-WSD, N.D. Georgia Dkt. No. 17-6, attached hereto as Exh. 12.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion for Summary Decision and ORDER that the Complaint be dismissed with prejudice.

Respectfully submitted,

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

Dated: April 21, 2014

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. 9357**
	)	
LabMD, Inc., **a corporation.**	)	**PUBLIC**

[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.'S MOTION FOR SUMMARY DECISION

This matter came before the Commission on April 21, 2014, upon a Motion for Summary Decisions ("Motion") filed by Respondent LabMD, Inc. ("LabMD") pursuant to Commission Rules 3.22 and 3.24, 16 C.F.R. §§ 3.22 and 3.24, for an Order granting summary decision in favor of LabMD on all counts set forth in the Federal Trade Commission's ("FTC") administrative Complaint against LabMD, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (Aug. 28, 2013). Having considered LabMD's Motion and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that LabMD's Motion is GRANTED.

ORDERED:

Edith Ramirez, Chairwoman
Maureen K. Ohlhausen
Joshua D. Wright
Commissioners

Date:

CERTIFICATE OF SERVICE

I hereby certify that on April 21, 2014, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I caused to be hand-delivered twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

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

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

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Jarad Brown, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

Dated: April 21, 2014

By: /s/ Michael D. Pepson
Michael D. Pepson

CERTIFICATE OF 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.

Dated: April 21, 2014 By:/s/William A. Sherman, II

EXHIBIT 1

In the Matter of:

LabMD, Inc.

November 21, 2013
Robert J. Boback

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

25

[redacted]

Q. When did Tiversa download CX 10?
A. I believe it was in February of 2008.
Q. Has CX 10 changed in any way since Tiversa downloaded it?
A. No.

[redacted]

A. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

EXHIBIT 2

Forthcoming in *Financial Cryptography and Data Security*, February 22-25, 2009.

Data Hemorrhages in the Health-Care Sector[1]

M. Eric Johnson

Center for Digital Strategies
Tuck School of Business
Dartmouth College, Hanover NH 03755
{M.Eric.Johnson}@dartmouth.edu

Abstract. Confidential data hemorrhaging from health-care providers pose financial risks to firms and medical risks to patients. We examine the consequences of data hemorrhages including privacy violations, medical fraud, financial identity theft, and medical identity theft. We also examine the types and sources of data hemorrhages, focusing on inadvertent disclosures. Through an analysis of leaked files, we examine data hemorrhages stemming from inadvertent disclosures on internet-based file sharing networks. We characterize the security risk for a group of health-care organizations using a direct analysis of leaked files. These files contained highly sensitive medical and personal information that could be maliciously exploited by criminals seeking to commit medical and financial identity theft. We also present evidence of the threat by examining user-issued searches. Our analysis demonstrates both the substantial threat and vulnerability for the health-care sector and the unique complexity exhibited by the US health-care system.

Keywords: Health-care information, identity theft, data leaks, security.

1 Introduction

Data breaches and inadvertent disclosures of customer information have plagued sectors from banking to retail. In many of these cases, lost customer information translates directly into financial losses through fraud and identity theft. The health-care sector also suffers such data hemorrhages, with multiple consequences. In some cases, the losses have translated to privacy violations and embarrassment. In other cases, criminals exploit the information to commit fraud or medical identity theft.

[1] Experiments described in this paper were conducted in collaboration with Tiversa who has developed a patent-pending technology that, in real-time, monitors global P2P file sharing networks. The author gratefully acknowledges the assistance of Nicholas Willey. This research was partially supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

EXHIBIT 3

In the Matter of:

LabMD, Inc.

December 17, 2013
Detective Karina Jestes

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

25

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

29

the document that's been produced as CX0085.
A Okay.
Q Are the documents that appear at CX0085 a true and accurate copy of the materials that you seized at [redacted] that referenced LabMD?
A Yes.
Q Are these the documents -- excuse me.
Are the documents that appear at CX0085 a true and accurate copy of the materials that you provided to FTC staff?
A Yes.
Q Did you book CX0085 into evidence?
A Yes.
Q Explain the process by which information collected during an investigation is booked into evidence.
A When an officer retrieves the evidence from a scene, basically, it's maintained under their control until it is then transported to the evidence section where it's inputted into a computer and then put into a locked container for the evidence technicians to then find a permanent place for.
Q That process occurred with respect to the document that appears at CX0085; is that correct?
A Yes.
Q Is booking into evidence information that an

30

officer collects, during a criminal investigation, done in the ordinary course of the Sacramento Police Department's activities?
A Yes.
Q I'm handing you a document that has been marked as CX0087.
(Exhibit CX0087 was marked for identification.)
BY MS. VANDRUFF:
Q I'm going to ask you to please take a moment to review that.
A Okay.
Q What is CX0087?
A "Day Sheet Transaction Detail" from LabMD, and it's marked that it's a copy, and then there's a number at the top that's the evidence control number for this document.
Q What is an evidence control number?
A When items of evidence are booked from the scene of the crime, they're each given a unique number; so this number is -- well, "755867" would be the kind of group number that items of evidence can be logged in under, and then each item is given a specific number; so this one is "6."
Q Can you tell whether CX0087 was booked into

31

evidence?
Let me ask the question differently, Detective Jestes.
Does the presence of the control number, 755867-6, tell you whether or not the document that has been marked as CX0087 was booked into evidence?
A Yes, it was.
Q Is the document that appears at CX0087 a true and accurate copy of the booked evidence, 755867, Item 6?
A Yes.
Q Did you book CX0087 in your ordinary course of your duties as a detective at the Sacramento Police Department?
A Yes.
Q I'm handing you a document that has been marked as CX0088.
(Exhibit CX0088 was marked for identification.)
BY MS. VANDRUFF:
Q I'm going to ask you to take a moment, please, and review the document.
A Okay.
Q What is CX0088?
A It's Item of Evidence No. 55867-7.
Q Was CX0088 booked into evidence?

32

A Yes.
Q Did you book CX0088 in the ordinary course of your duties as a detective of the Sacramento Police Department?
A Yes.
Q With respect to CX0088, is CX0088 a true and accurate copy of what you booked into evidence as 755867, Item 7?
A Yes.
Q I'm handing you a document that has been marked as CX0086.
(Exhibit CX0086 was marked for identification.)
BY MS. VANDRUFF:
Q I'm going to ask you to please take a moment and review the document.
A Okay.
Q What is CX0086?
A A declaration of custodian of records.
[redacted]

33

Q **Does CX0086 relate to Booked Evidence Case No. 755867?**
A Yes.
Q **Does CX0086 relate specifically to the documents that we have just discussed that appear at CX0087 and 0088?**
A Yes.
MS. HARRIS: Pardon me.
I'm going to interpose an objection that this witness is not the proper witness to lay a foundation for the records that we've just discussed. [redacted] is the proper person to lay the evidentiary foundation.
BY MS. VANDRUFF:
Q **Let's return to CX0087.**
What information is contained in CX0087?
A The top of the sheet says "Day Sheet Transaction Detail LabMD, Inc.," and then there is what appears to me to be names of possibly clients with social security numbers and then a billing number, a date, and then there's an amount -- a monetary amount.
Q **Based on your training and experience, where are the social security numbers that appear on CX0087?**
A To the left of the name.
Q **Why do you conclude that those are social security numbers?**

34

A Because there's three numbers, a dash, two numbers, a dash, and then four numbers, which in my training and experience is a social security number.
Q **Why did you book CX0087 into evidence?**
A Because I felt that there was evidence of identity theft.
Q **Based on your training and experience, what led you to that conclusion?**
A Part of identity theft is having the personal identifying information of another, and none of these people listed here or their social security numbers were supposed to be in that house. These documents are other people's identifying information. Ms. [redacted] and Mr. [redacted] should not have had possession of this.
Q **Did the presence of other documents that related to individuals who were neither Mr. [redacted] nor Ms. [redacted] affect your opinion about the significance of the document that appears at CX0087?**
A Sorry. Could you repeat that one?
MS. VANDRUFF: I'm going to ask the reporter to repeat that for me.
(Record read.)
THE WITNESS: Yes.
BY MS. VANDRUFF:
Q **In what way?**

35

A The other items that were found in this home such as checks and utilities with other people's information on them was also evidence of identity theft; so I believed that this information as well could have been used for financial gain or some kind of narcotics gain by these people by having other people's social security numbers and names in their possession.
Q **Okay. I'd ask you to return your attention please to the document that appears at CX0088.**
What information is contained in CX0088?
A These are copies of checks written to LabMD and signed by the person whose name is on the check.
Q **What types of personal information are included in the checks that appear in CX0088?**
A Names, addresses, phone numbers, account numbers, and signatures.
Q **In addition to the information that you've just described, there are handwritten notations on some of the pages -- for example, pages 4, 7, and 9.**
What is the significance of the notations that appear on pages 4, 7, and 9 of CX0088?
MS. HARRIS: Objection to the extent it calls for speculation.
THE WITNESS: It looks like there are social security numbers written on those checks.

36

BY MS. VANDRUFF:
Q **What is the basis of that conclusion?**
A Again, the way the number is written. There's three digits, a dash, two digits, a dash, and then four digits.
Q **In your training and experience, what's the significance of that sequence of numbers?**
A It would be a social security number.
Q **There are notations that appear on other pages -- for example, page 1, 5, and 8.**
What is the significance, if you know, of those notations?
MS. HARRIS: Objection. Calls for speculation.
THE WITNESS: Some of them look like monetary amounts, and then it looks like there's a phone number written on one, and I don't know -- I'd have to do more comparing of another documents to see if they correlated.
BY MS. VANDRUFF:
Q **Why did you book CX0088 into evidence?**
A These checks didn't have any connection to the house we were at or the people who were residing there at the time, and they should not have had in their possession account numbers and other personal identifying information from other people.
Q **So given that this -- that the document that**

53

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

56

MS. VANDRUFF: Objection to form.

THE WITNESS: Correct.

BY MS. HARRIS:

Q With respect to what has been marked by complaint counsel as CX0088 this morning, did you attempt to contact any of the people listed on these checks?

A From what I remember of my investigation, I looked and saw that none of them had a Sacramento connection based on their information on the checks, and I may have done a simple Google-type search to see if they had a connection, but since it's not documented in my report, there was no connection to these people to the Sacramento Police Department.

Q Do you have any evidence that any of the people in CX0088 have been the victim of identity theft?

A I do not have that information.

Q So the LabMD documents which, again, have been identified as CX0088 and CX0087 --

MS. VANDRUFF: Counsel, I'm sorry to interrupt. We've also marked as CX0085 the materials that Detective Jestes provided initially to FTC staff. Just so the record is clear, there are three separate exhibits that relate to LabMD.

Excuse my interruption.

EXHIBIT 4

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
	)	

COMPLAINT COUNSEL'S AMENDED RESPONSE TO LABMD, INC.'S FIRST SET OF REQUESTS FOR ADMISSION (NUMBERS 1-20)

Pursuant to Sections 3.31 and 3.32 of the Federal Trade Commission's Rules of Practice for Adjudicative Proceedings ("Rules of Practice"), Complaint Counsel hereby amends its responses to Respondent LabMD, Inc.'s First Set of Requests for Admission ("Respondent's Requests").

Complaint Counsel has not completed its discovery or its preparation for trial. Complaint Counsel's answers to Respondent's Requests are given without prejudice to Complaint Counsel's right to produce information relating to any subsequently discovered facts. Complaint Counsel reserves the right to assert additional objections to Respondent's Requests, and to amend or supplement these objections and responses as necessary after the close of discovery.

General Objections

The following General Objections apply to each of Respondent's Requests and are hereby incorporated by reference into each response. The assertion of the same, similar, or additional objections or the provision of partial answers in response to an individual Request does not waive any of Complaint Counsel's General Objections as to the other Requests.

Response to Request for Admission No. 5

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. *See* Order Denying Respondent LabMD's Motion to Dismiss at 14, *In the Matter of LabMD, Inc.*, Docket No. 9357 (Jan. 16, 2014) ("information security is an ongoing process of assessing risk and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve.") (citation omitted). Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "industry standards."

Complaint Counsel denies the Request to the extent that it suggests that Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), requires Complaint Counsel to allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use.

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel otherwise admits Request for Admission No. 5.

Request for Admission No. 6

Admit that the FTC has no evidence to dispute that LabMD has never been accused of violating either the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH) or any regulations implementing those statutes, including but not limited to as 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000) (HIPAA Privacy Rule); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (HIPAA Security Rule); 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013) (HHS HITECH rule).

Response to Request for Admission No. 6

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding. Complaint Counsel further objects to this Request to the extent it seeks information protected from disclosure by the common interest, deliberative process, law enforcement, and work product privileges. Complaint Counsel further objects to this Request to the extent it seeks information outside its possession, custody or control. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Request for Admission No. 7

Admit that the FTC has not accused LabMD of violating any rules or regulations not specifically referenced within the four corners of the FTC's Complaint.

Response to Request for Admission No. 7

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 7.

Request for Admission No. 8

Admit that HIPAA, HITECH, and regulations implementing those statutes are not mentioned in the FTC's Complaint.

Response to Request for Admission No. 8

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding.

Subject to and without waiving the foregoing objection and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 8.

Request for Admission No. 9

Admit that the information contained in the "Day Sheets" and "P2P insurance aging file" referred to in paragraphs 20 and 21 of the Complaint constitute Protected Health Information (PHI), as that term is used in HIPAA, HITECH, and regulations implementing those statutes.

Response to Request for Admission No. 9

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to this Request to the extent it seeks a legal conclusion regarding the application of HIPAA, HITECH and the regulations implementing those statutes.

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits that the information contained

EXHIBIT 5

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

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

EXPERT REPORT OF RAQUEL HILL, PH.D.

TABLE OF CONTENTS

EXPERT REPORT OF RAQUEL HILL, PH.D.

I. Introduction

1. I am a tenured professor of Computer Science at Indiana University with over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems.

2. The FTC has engaged me to testify as an expert in this litigation. As explained in more detail in Section V, below, Complaint Counsel has asked me to assess whether LabMD provided reasonable and appropriate security for Personal Information[1] within its computer network.

3. This report states my opinions and provides the justifications for those opinions. It also includes the following information:

- A summary of my experience and qualifications;
- An overview of network security principles and a description of LabMD's network; and
- A description of the materials that I considered in forming my opinions and conclusions.

4. Based on my review of the materials described in Section VI, below, and my experience described in Section II, below, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures. This conclusion covers the time period from January 2005 through July 2010

[1] For purposes of this report, Personal Information means individually identifiable information from or about an natural person including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. See Complaint Counsel's February 19, 2014 Requests for Admission to LabMD, p. 2.

(Relevant Time Period); as I explain in Paragraph 48, below, from my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period. In section VIII, below, I present my specific opinions that support this conclusion.

II. Summary of Experience and Qualifications

5. I have over 25 years of combined academic, research, and industrial experience in computing. I received my B.S. degree with Honors in Computer Science from the Georgia Institute of Technology. As an undergraduate, I worked as a Cooperative Education student with IBM and received my Cooperative Education Certificate for working a minimum of six academic quarters with IBM as an undergraduate. This cooperative education experience allowed me to apply the theories that I was learning in the classroom, but also enabled me to help fund my degree.

6. I also received my M.S. degree in Computer Science from Georgia Tech. As an M.S. student, I worked for several companies, including: Cray Research, Hayes Microsystems, and Nortel Networks. My M.S. degree was funded by Cray Research via an academic scholarship.

7. After completing my M.S. degree, I worked for three years with Nortel Networks, where I designed and implemented network protocols that enabled telephone switches to communicate with remote devices. These protocols sustained communications even when a communications channel failed.

8. In 1996, I left Nortel Networks to pursue a Ph.D. in Computer Science at Harvard University. At Harvard, I designed and implemented a quality of service protocol that enabled routers in the network to reserve bandwidth for audio and video applications using a light-weight signaling protocol. As a part of this work, I evaluated the protocol to determine the threats and

vulnerabilities and designed mechanisms to secure the reservation process. I received my Ph.D. in October 2002, and began working as a lecturer within the School of Electrical Engineering at the Georgia Institute of Technology, where I taught a course in Digital Circuits. After working at Georgia Tech for 9 months, I accepted a position as a Post-Doctoral Research Associate with a joint appointment in the Computer Science Department and the National Center for Super Computer Application (NCSA) at the University of Illinois, Urbana-Champaign. As a Post-Doc, I designed and implemented mechanisms to secure environments where mobile devices and sensors are an integral part of the computing space. These spaces are often referred to as pervasive or ubiquitous computing environments. One of the major challenges to securing such environments is to apply uniform security policies across devices that have varying computational, space, and battery limitations.

9. After completing a two-year assignment at the University of Illinois, I joined Indiana University as an Assistant Professor of Computer Science in 2005. I was promoted to Associate Professor with tenure in 2012. Over the years, I have designed and taught classes in information and systems security including: Analytical Foundations of Security, Trusted Computing, Computer Networks, and Data Protection. My research areas span the areas of system security and data privacy. I have published articles on various topics, including: quality of service in networking, security for pervasive computing environments, encryption-based access control, reputation systems, trusted computing, smartphone security, and privacy in research datasets. I have published over 25 peer-reviewed articles and abstracts and given 25 invited technical talks and panels.

10. I am currently on sabbatical at Harvard University, where I am a Visiting Scholar within the Center for Research on Computation and Society at the School of Engineering and Applied Sciences. I am continuing my data protection research with a specific focus on medical data.

11. A more extensive summary of my professional accomplishments and a list of all publications that I have authored within the last 10 years can be found in my *curriculum vitae*, a copy of which is attached to this report as Appendix A. I have not testified as an expert at trial or at deposition within the last four years.

12. I am being compensated at a rate of $150 per hour for my work in connection with this litigation.

III. Overview of Network Security Principles

A. Background: Computer Networks

13. In this section, I describe very basic network functionality at a high level to support my opinions. A network is a collection of workstations, laptop computers, servers, and other devices (computers) that are connected via some communications channel that is either wired or wireless. In commercial settings, data is usually passed between computers within a network via a switch or a router. A switch and router can be combined into one device.

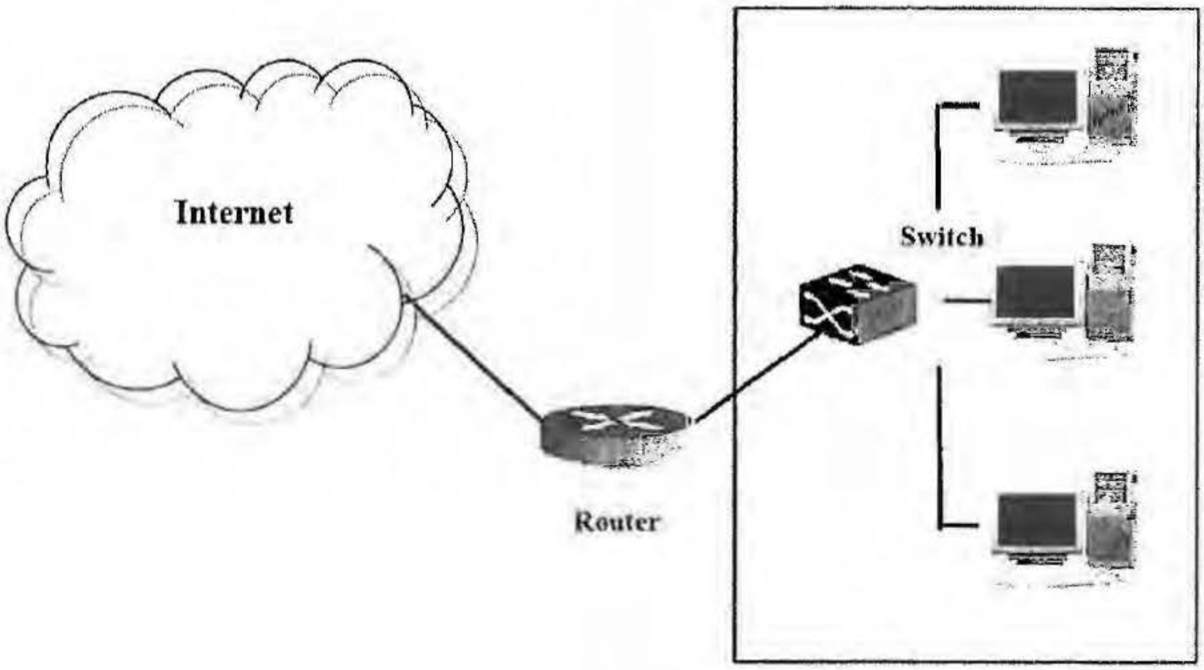
14. Computers use network interface cards (NIC) to connect to a network, and each NIC has a unique media access control (MAC) address. Each computer within a network is therefore uniquely identified by the MAC address of the computer's NIC. A computer's MAC address is not known outside of a computer's local area network (LAN).

15. A switch is a device that inspects incoming data to determine the destination MAC address and forwards the data to the computer with the specified MAC address.

16. A router is a device that connects networks. These networks may be of different types: wired vs. wireless, Ethernet vs. optical, etc. Routers forward data (in small units called packets) across the Internet using the Internet Protocol (IP) address of the destination computer. In doing so, the Domain Name System (DNS) is used to map a computer's hostname or a URL to an IP address. A computer's IP address is used by routers to forward data across the Internet to the specified destination network. Once the data reaches the destination network, the local switch uses the Address Resolution Protocol (ARP) to determine the MAC address of the computer that has the specified IP address. The switch passes the data to the destination computer.

17. **Figure 1** illustrates how a LAN may connect to the Internet. In the figure a switch connects the computers on the LAN and a router connects the LAN to the Internet. As noted in Paragraph 13, above, the function of the switch and the router can be combined into one device.

Figure 1: Connecting to the Internet



i. Network Addresses and Ports

18. In Paragraphs 13-16, I identified three types of addresses: Hostnames/URLs, IP addresses, and MAC addresses. DNS maps a hostname to an IP address, and ARP maps an IP address to a MAC address. The hostname and IP and MAC addresses are all needed to forward data to a specific computer. Once the data arrives at that computer, it must be sent to the application that is awaiting the information. The application is the ultimate recipient of any data that is sent to a computer on a network.

19. Applications are identified by numbers called ports. When data arrives at the destination, the receiving computer extracts the port number from the data and sends the data to the application that corresponds to that port number. Applications and their corresponding port numbers are the doors to computers and the networks to which the computers are connected. An application that contains a security vulnerability may allow an external entity to gain access to the LAN and any resources that are connected to the LAN. For this reason, it is important to ensure that all computers have been updated with all of the latest security patches for applications and related software

20. There are $2^{16} = 65,536$ possible ports on any computer. An open port is an open door to the computer, even when there is no application attached to the port. Therefore, it is important to close all unused ports on all computers. For example, when web access is not approved or authorized, ports 80 and 443 (which are typically used for web access) should be closed to prevent access to the computer through those ports.

ii. Firewalls and Intrusion Detection Systems

21. Firewalls are barrier mechanisms that are used to protect networks and individual computers. A firewall can be either a hardware device or a piece of software. It can be placed at a network gateway, or installed on a router or individual computer.

22. Firewalls can be configured to close all unused ports. When a port is closed, any data that arrives at the network or computer for that port will be discarded. Firewalls can also be configured to prevent and/or limit incoming connection requests. An incoming connection request is a request that originates from outside of the network but seeks to establish communication with a computer that is within the network. Only computers that are running authorized server applications should receive connection requests. A firewall, for example, could be configured to prevent all incoming connection requests for computers that are not running an authorized server application.

23. An intrusion detection system (IDS) is a device, typically another computer, that is placed inside a protected network to monitor activity in order to identify suspicious events. It can be either host-based or network-based. A host-based IDS runs on a single computer to protect that one host, while a network-based IDS is a stand-alone device that is attached to the network to monitor traffic throughout the network. An IDS acts as a sensor, like a smoke detector, that raises an alarm if specific things occur. It may perform a variety of functions including: monitoring users and system activity; auditing system configuration for vulnerabilities and misconfiguration; assessing the integrity of critical system and data files; identifying known attack patterns in system activity; recognizing abnormal activity through statistical analysis; managing audit trails and highlighting user violations of policy; correcting system configuration errors; and installing and operating traps to record information.

iii. Authentication and Access Control

24. Authentication and access control mechanisms prevent unauthorized access to computers, applications, services, and data.

25. To authenticate themselves, users provide a combination of information that tells the system who they are (identity) and information that proves that identity (proof). Usernames and passwords are commonly used to authenticate users. When authenticating, a user enters her username to identify herself to the authentication system, and her password to prove her identity. Some authentication mechanisms may require multiple forms of proof. For example, a user may be required to provide a password (what she knows), and proof of using something she possesses, such as a biometric (finger print, iris scan, etc.) or token. An authentication mechanism that requires two forms of proof is called two-factor authentication, and it is used as part of a defense in depth strategy (see Section III.B below) to reduce the risk of compromise. Remote login and access to highly sensitive data are scenarios for which either two-factor or multi-factor authentication is often used.

26. Access control mechanisms restrict a user's access to computers, services, applications, or data. An access control mechanism enforces policies that specify the resources that users may access. A user's role, security clearance, etc., may be used to identify the resources to which that user has access.

B. Defense in Depth

27. The most effective way to secure a network and its computers is by using multiple security measures to provide defense in depth. In such an approach, the network is viewed as a system with multiple layers, and security mechanisms are deployed at each layer to reduce the overall likelihood that an attack will succeed. The basic idea is not to rely on just one security

measure. Practicing defense in depth reduces the likelihood that an attack will succeed by forcing the attacker to penetrate multiple defenses. To generally illustrate the benefit of defense in depth, assume that an attacker has a 50% chance of penetrating each defense mechanism. If there are three layers of protection, the probability of gaining unauthorized access to a resource at the innermost layer is $(1/2)^3 = 1/8$.

28. To illustrate the concept of network layers and defense in depth, consider Figure 1 above. In this simple network, the layers are: the router that connects the LAN to the Internet; the computers on the LAN; and applications on each computer on the LAN. Defense in depth on this network would require security policies and mechanisms to be specified and deployed at the router that connects the LAN to the Internet, at the workstations/servers, and at user accounts on those computers.

29. Continuing with the simple network in Figure 1, assume there is a risk that a company's employees will download and install on their computers applications they do not need to perform their jobs and that the company has a security policy prohibiting unauthorized applications. A simple prohibition that relies on employees following the policy does not provide defense in depth. A defense in depth strategy would prevent the employee from installing the application and/or limit the impact of an unauthorized application on the network. To achieve defense in depth, the company should use different security measures at different layers in the network, as follows:

a. **Internet Connection Layer:** At this layer, we cannot prevent software from being installed on a workstation or server, but we can restrict the type of traffic that flows into the network. Therefore, even if unauthorized software has been inadvertently installed on a workstation/server, mechanisms could be used to render the application ineffective. Recall that port numbers map to specific applications, and that firewalls can be configured to restrict the types of application traffic that is allowed into the network, by dropping any data that contains an unauthorized port number. Thus, to illustrate the concept of defense in depth, a first line of defense to prevent use of unauthorized applications is to configure a firewall to close all ports at the gateway router except those that are used by authorized applications. Other mechanisms besides firewalls could be deployed at this layer as well, such as an IDS.[2]

b. **Workstation/Server Layer:** Even if a firewall were deployed at the gateway router, a second layer of security may be appropriate. The firewall at the gateway router may be misconfigured or not configured to discard all unauthorized traffic because the corresponding firewall policy would be hard to implement and manage. In these circumstances, a software firewall can be deployed at workstations and servers to further filter traffic that may have passed through the firewall at the gateway router. Because the firewall at a workstation or server is configured to protect that specific computer, the security settings can be more restrictive.

c. **User Account Layer:** Finally, in the simple network in Figure 1, user accounts for specific computers could be configured to so that system administrators can install software but ordinary users cannot.

30. As illustrated above, deploying security measures at different layers of a network enhances overall security by closing gaps in any one measure. In practice, achieving defense in

[2] A firewall and IDS could be used together to provide additional protection. If an IDS detects a violation, it could send a security alert to the system administration, indicating that unauthorized traffic is entering the network (i.e. traffic destined for an unauthorized application) and that firewall settings need to be updated to discard such traffic.

depth involves using layered security measures to address the many different risks and vulnerabilities a network may face.

C. Principles for Assessing and Securing a Network

31. There are seven principles that help to specify the policies and identify the mechanisms that are to be deployed at each layer of a defense in depth security strategy. These principles are listed and described below.

a. **Don't Keep What You Don't Need:** The first principle recognizes that maintaining sensitive information that is not needed creates an unnecessary risk.

b. **Patch:** A most basic principle is to Patch, meaning to apply updates to fix all known or reasonably foreseeable security vulnerabilities and flaws.

c. **Ports:** The third principle concerns Ports. As previously stated, applications communicate via ports. There are well-known ports for well-known applications. For example, a web server listens for incoming connections on Ports 80 and 443. All unused ports should be closed.

d. **Policies:** Policies are processes and procedures that are put in place to satisfy an organization's security requirements. Examples of policies would include the following:

- **Data Access** – Limit data access to persons with a need for the data.
- **Passwords** – Policies regarding passwords should contain rules about the following:
  - Acceptable minimum length.
  - Lifetime of a password.
    - The lifetime of a password is often related to the sensitivity of the information that the user accesses, the greater the sensitivity, the shorter the password's lifetime.
  - Password history.

- Passwords to avoid.
  - If you are a big sports fan, don't use a password that is related to your favorite team.
  - Avoid personal data such as spouse's name, children's name, pet's name, and birthdays.

- **Backups** – Backup data on a regular basis to be able to restore it because data is more valuable than the computer.
  - Encrypt backups.
  - Keep data in a secure location.
  - Limit access to backups.

e. **<u>Protect</u>:** Ensure that reasonable security software is employed, such as firewalls, anti-spyware, anti-virus, and IDS software, and authentication and access control. This list includes software that can be classified as either proactive or reactive. Proactive mechanisms attempt to prevent threats, while reactive mechanisms respond to threats that may have bypassed proactive mechanisms. Therefore, both types of mechanisms should be used to secure a system. Firewalls, authentication, and access control mechanisms try to block or prevent attacks. Anti-spyware, anti-virus, and IDS mechanisms attempt to detect the presence of malicious software or an attack while it is occurring.

f. **<u>Probe</u>:** Probing is a security audit that tests the state of a network. One type of probing is penetration testing, which searches the network for security flaws. Penetration testing includes scanning ports to verify that unused ports are closed or disabled. A thorough security probe would include a review of security policies, patching system, security logs, computers for unauthorized software, and any other processes, procedures, or information that may impact the security of a system.

g. **Physical:** There must be policies that govern the physical access to devices and data. Some examples of such policies include:

- Computer rooms must be locked.
- Server rooms must be locked with limited access.

IV. LabMD's Network During the Relevant Time Period

32. LabMD's network was small and simple. It included: computers LabMD provided to physician clients to use to place orders and retrieve results over the Internet; a small number of servers located at its business premises; and computers used by employees. In this section, I describe at a high level the network during the Relevant Time Period.

33. LabMD provided computers to physician clients. Through these computers, physician clients sent Personal Information over the Internet to LabMD. This information included names, addresses, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and services, and other information. In some instances, physician clients entered the information into the computer that LabMD had provided, one consumer at a time, and then sent the information to LabMD. In other instances, the LabMD computer in the physician's office retrieved Personal Information for all patients of the physician's practice from a database located on another computer in the physician's office and forwarded the information for all of those patients in bulk to LabMD, regardless whether LabMD performed testing for those patients.

34. The Personal Information LabMD received from physician clients typically was transmitted from physician clients to LabMD's network using a File Transfer Protocol (FTP) service LabMD installed on its network and the computers it provided to physician offices.

35. Regardless of whether Personal Information came as a bulk transfer or one consumer at a time, it was received by a server on LabMD's network (called Mapper), where it was processed (so that it could be used by applications LabMD used in is laboratory and billing department) and

then maintained on servers on the network. The laboratory and billing applications also ran on servers on LabMD's network. In addition, LabMD maintained Personal information on desktop computers, such as the Finance/Billing Manager's computer.

36. After LabMD's laboratory and medical employees had provided the services ordered by physician clients, they added results to the Personal Information LabMD maintained on its network.

37. The evidence in the record shows that LabMD did not encrypt Personal Information while it was maintained on LabMD's network.

38. Physician clients typically retrieved the results of the services they ordered from LabMD through LabMD's web portal. In doing so, they accessed Personal Information stored on LabMD's network.

39. LabMD's network included a number of servers that hosted applications, including back-up, email, webserver, database, laboratory, and billing applications. Some of these servers hosted multiple applications and also stored Personal Information. For example, one server hosted billing and mail applications [3]

40. Employees in the laboratory and billing departments, and certain other employees, used their LabMD computers to access resources on LabMD's network, including applications that provided access to Personal Information maintained on the network. Some LabMD employees could remotely access LabMD's network, including Personal Information maintained on the network.

[3] See, for example, FTC-LABMD-00002 (CX0034).

41. Record evidence shows that in 2005 or 2006, LimeWire, a peer-to-peer (P2P) file-sharing program, was installed on a computer on LabMD's network. The computer was used by the Billing Manager.

42. At a high level, the software is called peer-to-peer because users use it to search for and retrieve files directly from the computers of others using the software instead of retrieving files from a central server. To do this, the software allows users to designate or place files they will share in a folder (Sharing Folder). Using the software, a user can search the Sharing Folders of other users for files of interest. P2P programs have been widely available since 1999, and have been, and are, used by millions of users to share music, video, and other types of files.

43. Record evidence, including a screenshot of the Sharing Folder on the Billing Manager's computer taken in May 2008, shows that hundreds of files were in the Sharing Folder on the Billing Manager's computer.[4] Among these files was an insurance aging file (called the 1,718 File) that contained Personal Information about more than 9,300 people.[5] Copies of the 1,718 File were found on computers in California, Arizona, Costa Rica, and the United Kingdom.[6]

44. The risk of inadvertently sharing files with sensitive information using P2P software and the difficulty of undoing sharing are well known. After a file has been shared, the copy is out of the control of the original source and can be shared again from its new location to any number of other computers running the software. Searching for the file might not find all of the copies

[4] See FTC-LABMD-3755 (CX0152).

[5] See FTC-LABMD-3755 (CX0152); Tiversa-FTC_Response-000001 through Tiversa-FTC_Response-001719 (CX0008)

[6] See Robert Boback, November 21, 2013 Deposition Transcript, pp. 50-53; TIVERSA-FTC_RESPONSE-000001 through TIVERSA-FTC_RESPONSE-006876 (CX0008-CX0011); TIVERSA-FTC_RESPONSE-006882 (CX0019).

because, for example, a computer with a copy might be turned off when the search occurs. Security professionals and others have warned about this risk since at least 2005.

V. Scope of Opinions

45. Complaint Counsel has asked me to assess whether LabMD provided reasonable and appropriate security for Personal Information within its computer network. Specifically, I was asked to analyze the record evidence relating to the following paragraphs of the FTC's complaint:

a. Paragraph 10: "At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:

- (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;
- (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;
- (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- (d) did not adequately train employees to safeguard personal information;
- (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;
- (f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely

that the systems would bc updated to address newly discovered vulnerabilities; and

- (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks."

b. Paragraph 11: "Respondent could have corrected its security failures at relatively low cost using readily available security measures."

VI. Materials Considered in Forming Opinions

46. A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B. Those materials include: transcripts and exhibits from investigational hearings and depositions of LabMD, its current and former employees, and third parties; documents and correspondence provided to Complaint Counsel by LabMD and third parties in connection with the pre-complaint investigation or this litigation; and industry and government standards, guidelines, and vulnerability databases that establish best practices for information security practitioners. I also have relied upon my education and experience in reaching my opinions.

47. I am continuing to review material obtained by Complaint Counsel through discovery in this litigation. LabMD produced to Complaint Counsel more than 11,500 pages of documents between February 25 and March 4, 2014, and Complaint Counsel has informed me that depositions are noticed to be taken after March 18, 2014. I reserve the right to revise or supplement my opinions based upon my continued review of the documents recently produced by LabMD, information learned during depositions conducted after the submission of this report,

or any other new information relevant to this litigation that comes to my attention after the submission of this report.

48. As I noted in Paragraph 4, above, my overall conclusion and the specific opinions that support that conclusion cover the Relevant Time Period, which is January 2005 through July 2010. From my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.

VII. Summary of Opinions

49. Based on my review of the materials described in Section VI, above, and my experience described in Section II, above, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures. In reaching this conclusion, I have taken into account the amount and nature of the data maintained within LabMD's network, LabMD's network and security practices, risks and vulnerabilities on LabMD's network, and the cost of remediating those risks and vulnerabilities. Record evidence shows that LabMD maintains Personal Information about more than 750,000 consumers.[7] For purposes of this report, I have assumed that these types of information can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information.

50. In Section VIII, below, I present my specific opinions that support my overall conclusion. In each subpart of Section VIII, below, I present my specific opinions regarding whether LabMD

[7] See LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 23. For most of those consumers, that information includes: Social Security numbers, insurance information, and medical diagnosis codes. See Tiversa-FTC_Response-000001 through Tiversa-FTC_Response-001719 (CX0008).

could have corrected its security failings at relatively low cost using readily available security measures, which relate to Paragraph 11 of the Complaint.

VIII. Opinions

A. Comprehensive Information Security Program – Complaint ¶ 10(a)

51. Complaint Counsel has asked me to provide an opinion on whether LabMD developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information. My opinion is organized as follows: (1) an explanation of the contents of a comprehensive information security program; (2) my opinion, including some examples of key evidence supporting those opinions.

52. A comprehensive information security program is a plan that sets out an organization's security goals, the written policies that would satisfy those goals, the mechanisms that would be used to enforce the written policies, and how those mechanisms would be used to enforce the written policies. The best practices for developing a comprehensive information security program would include the seven principles that I discuss in Paragraph 31, above: don't keep what you don't need, patch, ports, policies, protect, probe and physical.

53. A comprehensive information security program should be in writing to provide guidance to those who are implementing the plan and those who receive training through the plan. It also should be in writing to record the organization's current security goals and practices to facilitate changes to those goals and practices as security threats continually evolve and, because turnover is inevitable, to communicate the security goals and practices of the organization to future employees.

54. An organization's comprehensive information security program should specify confidentiality, integrity, and availability goals, and related policies and mechanisms.

55. A confidentiality goal/policy ensures that only authorized individuals are able to access data. Encryption and access controls are mechanisms that can be used to enforce confidentiality policies. Encryption mechanisms are used to protect stored data and data that is being transmitted between parties, but encryption alone doesn't prevent unauthorized individuals from gaining access to the data. If I encrypt the data and distribute the encryption key to everyone, the encryption procedure is ineffective. Therefore, in addition to encrypting the data, an organization should specify under which conditions should data be accessed and which employees should be allowed to access the data. Role-based access control policies have been often used by organizations to differentiate the data access of employees. In such policies, employees are assigned data access rights based on the job that they are required to perform.

56. An integrity goal/policy ensures that data is not inadvertently changed or lost. Mechanisms that enforce an integrity policy ensure that any unauthorized changes to a system and its data can be detected. For example, cryptographic hash functions may be used to detect unauthorized changes to stored data (i.e. software executables, patient records) and transmitted data. A cryptographic hash function takes data input of any size and computes a fixed-size number called a hash value that is unique to the data and can be used as the digital fingerprint for the data. Thus, changes in a file's hash value indicates that the file has been changed. Integrity-based software scanners can be configured to detect newly added software and/or changes to existing application executables. Any new software that has been installed on a computer may indicate an unauthorized installation, while changes to existing executables may denote that malware has been embedded in an application.

57. An availability goal/policy specifies processes to ensure that the computing system (i.e. hardware, software, and network), and data are accessible, even in the presence of natural disasters or malicious attempts to compromise the system.

58. Achieving confidentiality, integrity, and availability goals may incorporate the use of a variety of security mechanisms, including firewalls, intrusion detection systems, integrity scanners, anti-virus scanners, backups, logging, authentication, physical security, access control, risk assessment, and remediation, etc.

59. While security goals, policies and mechanisms are key components of any security plan, the success of any defense-in-depth based information security program will be limited when the users and managers of the computing system are not properly trained. Therefore any comprehensive security plan should also include training procedures for non-IT and IT employees. This training should ensure that employees understand the security goals and policies and how to use any mechanisms that are to be used to secure the system. In addition, IT staff should receive training on specific mechanisms to mitigate risks and on evolving threats. I discuss the training component of a comprehensive information security program in more detail in Section VIII.D, below.

60. Securing electronic health data is a topic that has been explored by many national experts for years, which has resulted in the creation of best practices and guidelines for securing this information. Examples of comprehensive information security programs concerning electronic health data have been available online at no cost from various sources since as early as 1997, including, for example, the National Research Council (NRC), the National Institute of Standards and Technology (NIST), and the Health Insurance Portability and Accountability Act

(HIPAA) Security Rule.[8] These comprehensive security programs include guidelines for ensuring the confidentiality, integrity, and availability of data, including mechanisms for authenticating individual users, employing access control mechanisms to restrict access based on an individual's role, limiting a user's ability to install software, assessing risks and vulnerabilities, encrypting stored data and data in transit, logging access to data and system components, ensuring system and data integrity, protecting network gateways, maintaining up-to-date software, etc.

61. Based on my review of evidence from the record, I have formed the opinion that LabMD did not develop, implement or maintain a comprehensive information security program to protect consumers' Personal Information. Record evidence shows that:

a. From 2005 to 2010, LabMD had no written information security program.[9] During the Relevant Time Period, LabMD employees received an employee handbook, but this document did not address the practices covered by a comprehensive security program. For example, the handbook states that LabMD has taken specific measures to comply with HIPAA but does not explain those measures.[10]

[8] See, for example, National Research Council, For the Record: Protecting Electronic Health Information (1997), at http://www nap.edu/openbook.php?record_id=5595&page=R1; Woody, Carol, Clinton, Larry, Internet Security Alliance, "Common Sense Guide to Cyber Security for Small Businesses" (March 2004), http://isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf; SANS Institute InfoSec Reading Room, "The Many Facets of an Information Security Program" (2003), https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343; and Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

[9] LabMD's Policy Manual, FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006) and LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual, FTC-LABMD-003590 through FTC-LABMD-003621 (CX0007), were written in 2010. See, for example, John Boyle February 5, 2013, Investigational Hearing Transcript, pp. 78-79, 91-92.

[10] See FTC-LABMD-003531 through FTC-LABMD-003553 (CX0001), p. 6; FTC-LABMD-003554 through FTC-LABMD-003575 (CX0002), p. 6.

b. Although LabMD contends that the policies set forth in LabMD's Policy Manual[11] were in place in 2007 and 2008, there is no documentation demonstrating that those policies were in place, and if they were in place, at least some of those policies were not being enforced. For example:

- LabMD contends that it adopted policies in 2002 to identify and remove unauthorized software that had been installed on employee computers and to configure firewalls on employee computers to block incoming connection requests. If these policies had been implemented, unauthorized software would have been detected and removed from employee computers, and computers located outside LabMD's network would not be able to initiate communications with computers inside the network. As discussed in Paragraphs 41-43, above, LimeWire, an unauthorized P2P file sharing program, was installed on the Billing Manager's computer in 2005 or 2006 and used to share files. LabMD's processes did not detect the software or prevent its use. LabMD removed the software in May, 2008, approximately two to three years from the date of installation, after being informed that the 1,718 File was found on a P2P network.
- In 2007 and 2008, when LabMD contends that the policies in its Policy Manual were in place, LabMD did not provide the encryption tools listed in its policy or provide staff with training on how to secure sensitive information included in emails or attachments.[12]

c. LabMD's Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual,[13] both of which were written in 2010, are not sufficiently comprehensive. For example, they lack specific policies that describe how Personal Information is protected during transmission between the physician offices and LabMD, and whether sensitive information is to be stored in an encrypted format.

[11] See FTC-LABMD-003141 through FTC-LabMD-003162 (CX0006); John Boyle February 5, 2013, Investigational Hearing Transcript, pp. 91-92.

[12] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 277-278; Alison Simmons May 2, 2013 Investigational Hearing Transcript, p. 163.

[13] See FTC-LABMD-003141 through FTC-LabMD-003162 (CX0006); FTC-LABMD-003590-3621 (CX0007).

- LabMD relied on the Secure Socket Layer (SSL) Protocol and HTTPS to encrypt communications and secure its web-based applications.[14] Record evidence shows that LabMD's servers allowed the use of SSL version 2.0, which had known security flaws.[15]

62. LabMD could have developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information at relatively low cost.[16]

B. Risk Assessment – Complaint ¶ 10(b)

63. Complaint Counsel has asked me to provide an opinion as to whether LabMD used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network, which is often called "risk assessment" in the IT field. My opinion is organized into several parts: (1) an explanation of why risk assessment is important; (2) a discussion of the mechanisms and protocols IT practitioners use to assess risks; and (3) my opinion, including some examples of key evidence supporting those opinions.

64. The relationship between risk assessments and reasonable security is very well known among IT practitioners, and frameworks for conducting risk assessments are widely available from many sources. When an assessment is inadequate or incomplete, network administrators and users may not know which risks or vulnerabilities they face and thus the security measures they should consider implementing. To IT practitioners, risk assessments are the foundation for choosing security measures that are reasonable and appropriate under their circumstances. It is an essential component of defense in depth.

65. IT practitioners use a variety of measures and techniques, to assess and remediate risks. These include antivirus applications, firewalls, various types of vulnerability scans, intrusion

[14] SSL is the protocol that ensures that data is encrypted for HTTPS.

[15] This vulnerability is discussed in Paragraph 100, below.

[16] See, for example, footnote 8, above, and the accompanying text.

detection systems, penetration tests, file integrity monitoring, and other measures. Typically, each mechanism can only assess the exposure to a particular type of risk or vulnerability. Antivirus applications, for example, can assess the incidence of viruses on a network, but not the installation of unauthorized applications on the network. Logs from firewalls, for example, can be reviewed to identify the application and host targets of unauthorized attempts to access the network, but traditional firewalls are designed to block specific types of traffic, not detect intrusions and attacks. An IDS can be used to detect attacks and alert the IT staff that firewall settings should be reconfigured. External vulnerability scans, which are conducted from outside the network, can, for example, assess the incidence of vulnerabilities in an application inside the network, but not the incidence of viruses. File integrity monitoring can identify changes in critical files that may indicate malware has been installed on the network, but does not identify or remove the malware. No one mechanism can assess the exposure to all the risks and vulnerabilities a network may face. An appropriate risk assessment process usually requires the use of a number of mechanisms.

66. Network administrators usually have a number of options to choose from in each mechanism category. For example, there are a number of branded antivirus applications, and within a brand there often are versions that differ in cost, the types of functions they can perform, and other aspects of performance. Properly used and reviewed, these mechanisms provide network administrators with essential information about risks and vulnerabilities they face. Having options provides companies with flexibility, so that they can balance the effectiveness of a mechanism, the sensitivity of the business and consumer information the assessment concerns, and the mechanism's cost.

67. Based on my review of the evidence from the record, I have formed the opinion that LabMD did not use an appropriate set of readily available measures to assess risks and vulnerabilities to the Personal Information within its computer network during the Relevant Time Period.

68. Record evidence shows that, prior to 2010, LabMD used antivirus applications, firewalls, and manual computer inspections to assess risks within the network. These mechanisms were not sufficient to identify or assess risks and vulnerabilities to the Personal Information maintained on LabMD's computer network.

a. As I discussed in Paragraph 65, above, antivirus applications can assess the incidences of viruses on a network but cannot assess the installation of unauthorized applications on the network. The evidence shows that at times, LabMD did not effectively manage its antivirus applications, or used applications that were out of date or had limited risk assessment functionality. For example, at some points, the antivirus application LabMD used on critical servers would not scan for viruses,[17] and thus could not identify risks to the servers. LabMD continued to use the same antivirus application after the vendor stopped providing updated virus definitions needed to identify newly discovered risks. On employee workstations, LabMD at times used antivirus applications that provided only limited risk assessment functionality, at least until late 2006. These applications could not be centrally managed by a network administrator; which meant that to be effective, individual employees had to update the virus definitions on their

[17] See, for example, FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035).

computers and report warnings to LabMD's IT Department. Even after it implemented a more capable antivirus application, LabMD did not install it on all its equipment.[18]

b. The firewall product that LabMD used until 2010 had very limited risk assessment capabilities. It could only log a few days of network traffic, which LabMD only reviewed to troubleshoot a performance problem, such as a user complaint that he or she could not connect to a website.[19] The firewall product also could not monitor traffic.[20] IT practitioners use traffic monitoring to, for example, determine if sensitive consumer information is being exported from their networks. LabMD could have used the freely available mechanism, Wireshark, to do packet level analysis to provide information to use to determine if Personal Information left the network without authorization.

c. Evidence in the record shows that, through at least mid-2008, LabMD conducted manual computer inspections only in response to a physician or employee reporting that a computer had malfunctioned.[21] Even when conducted on a regular basis, manual computer inspections can never be exhaustive because vulnerabilities and risks can exist anywhere in a computer, and human beings cannot inspect every one of those places. Even if they could, malicious software may, in some instances, mask its presence to avoid detection during a manual inspection, such as by altering the task manager application in Windows to prevent the malicious software's process from being displayed. For these reasons, IT practitioners should not rely on manual inspections and

[18] See, for example, Christopher Maire January 9, 2014 Deposition Transcript, p. 95; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 150-151.

[19] See, for example, Allen Truett February 27, 2014, Deposition Transcript, pp. 68-69.

[20] See, for example, Allen Truett February 27, 2014, Deposition Transcript, p. 67.

[21] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 177-178; Alison Simmons Investigational Hearing Transcript, pp. 78-80, 85-86; Matthew Bureau January 10, 2014 Deposition Transcript, pp. 50-52.

should also use automated mechanisms, such as IDS, file integrity monitoring, and penetration testing to assess risks and vulnerabilities on the network.

69. LabMD did not implement an IDS or file integrity monitoring,[22] and only began conducting penetration tests in May 2010. These tests were limited to external facing servers and did not test employee workstations and computers inside LabMD's network. LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using these automated mechanisms.

70. A penetration test of all IP addresses on the network, for example, would have identified vulnerabilities like outdated software, security patches that had not been applied, administrative accounts with default settings, etc. IT practitioners use this information to address these vulnerabilities. Information from penetration tests also could have identified all open ports within the network and all computers that accepted connection requests. This information could have been used to re-configure firewalls to close unneeded ports and to deny connection requests for computers whose work purpose didn't require the servicing of such requests.

71. Several well-respected and freely available penetration test and network analysis mechanisms have been available since 1997. Examples include: nmap (www.nmap.org, released 1997), Nessus (free until 2008), and Wireshark (formerly Etheral, released 1998). Using these mechanisms, LabMD could have conducted vulnerability scans, or had vulnerability scans conducted for it, throughout the Relevant Time Period, and doing so would have allowed it to correct significant risks, including those I describe in Paragraph 72, below, much sooner. The

[22] LabMD could have implemented an IDS and file integrity monitoring during the Relevant Time Period at relatively low cost. For example, LabMD could have implemented SNORT, a well-respected and widely used IDS that has been freely available since 1998, and, as I explain in Paragraph 104 below, Stealth and OSSEC are examples of freely available file integrity monitoring products.

cost of having penetration tests is modest: the penetration test LabMD had performed in 2010 by ProviDyn, an IT service provider, cost $450.[23]

72. Evidence in the record shows that the external vulnerability scans conducted in 2010 identified a number of well-known and significant risks and vulnerabilities on LabMD's network, including some that had been known to IT practitioners for years. For example, ProviDyn's April 2010 external vulnerability scan report identified a Level 5 anonymous FTP problem. This problem was first reported by the security community on July 14, 1993, 17 years before ProviDyn found it on LabMD's Mapper server.

73. Under the IT industry standardized classification system ProviDyn used, a Level 5 risk is an Urgent Risk and requires immediate remediation.[24]

74. The process for choosing reasonable and appropriate measures to address risks discovered through risk assessment is well-known and understood among IT practitioners and businesses. Guidelines on how to select reasonable and appropriate security measures have been freely available for years. NIST, for example, published a standard that explained the process in 2002.[25] In 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central

[23] See, for example, FTC-LABMD-003732 through FTC-LABMD-003736 (CX0044); FTC-LABMD-005254 through FTC-LABMD-005258.

[24] The risk classifications ProviDyn used are the classifications in the PCI Data Security Standard, which are derived from the Common Vulnerability Scoring System (CVSS) established by the National Institute of Standards (NIST). See PCI Technical and Operational Requirements for Approved Scanning Vendors, Version 1.1 (September 2006). In this classification, there are 5 levels: Urgent Risk (5), Critical Risk (4), High Risk (3), Medium Risk (2), and Low Risk (1). Level 5 (Urgent Risk) Vulnerabilities provide remote intruders with remote root/administrative capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers with full file-system read and write capabilities, remote execution of commands as an administrative user.

[25] See NIST Risk Management Guide for Information Technology Systems SP-800-30 (July 2002), at http://csrc nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

principles of NIST SP 800-30 in explaining how to perform the risk analysis and risk management required by the HIPAA Security Rule.[26]

75. IT practitioners have used these concepts to identify security measures that are reasonable and appropriate under various circumstances for years. The basic idea is to balance the severity of a risk and the harm that will result if the risk is exploited against the cost of a measure that remediates the risk. The more sensitive the Personal Information maintained within the network, the greater the need for enhanced security measures,

76. Consider the anonymous FTP problem set out in Paragraph 72, above: users are anonymous because no password is needed to log into the FTP service. It is an urgent risk to an application that LabMD used to transmit large amounts of Personal Information. Thus, the risk is high and the harm that would result if the risk were exploited is also high. The cost of remediating it is low, involving only IT-employee time to disallow anonymous log-ins. As a result, it would be reasonable and appropriate under these circumstances to disallow anonymous log-ins. The point of conducting appropriate risk assessments is to identify risks early, so that they can be remediated.

77. LabMD could have used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network at relatively low cost.[27]

C. Access to Information Not Needed to Perform Jobs – Complaint ¶10(c)

78. Complaint Counsel has asked me to provide opinions as to (1) whether LabMD maintained more Personal Information than necessary on its network and (2) whether LabMD

[26] See U.S. Department of Health and Human Services, HIPAA Security Series, "6 Basics of Security Risk Analysis and Risk Management" (March 2007), http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

[27] See, for example, Paragraph 71, above.

used adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs. My opinion is organized as follows: (1) an explanation of why it is important for an organization to not maintain more Personal Information than necessary on its network; (2) my opinion concerning whether LabMD maintained more Personal Information than necessary on its network, including some examples of key evidence supporting those opinions; (3) an explanation of why limiting access to Personal Information is important; (4) a discussion of the mechanisms IT practitioners use to limit access to information maintained within a network; and (5) my opinion concerning whether LabMD used adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs, including some of the evidence I considered.

i. Whether LabMD Maintained More Personal Information than Necessary

79. One of the principles of information security is for an organization to not maintain more information than it needs to conduct its business. This is important because, if an organization collects more data than is needed to conduct its business, it increases the scope of potential harm if the organization's network is compromised.

80. Based on my review of evidence from the record, I have formed the opinion that LabMD collected and maintained Personal Information about individuals for whom it has not performed testing (either directly or by outsourcing to another laboratory) and therefore did not use adequate measures to prevent employees from having access to Personal Information that was not needed to perform their jobs.

a. Record evidence shows that LabMD collected and maintained indefinitely Personal Information about approximately 100,000 consumers for whom it never performed testing (either directly or by outsourcing to another laboratory) and that

LabMD did not need to maintain Personal Information about those consumers in order to conduct its business.[28]

b. LabMD could have purged the data that it collected from consumers for whom it did not perform testing (either directly or by outsourcing to another laboratory) through its database applications. Purging data from a network is the type of thing that IT practitioners did regularly throughout the Relevant Time Period. Correcting this issue would have required only the time of trained IT staff and could have been done at relatively low cost.

ii. Whether LabMD Used Adequate Measures to Prevent Employees from Accessing Personal Information Not Needed to Perform Jobs

81. By not limiting access to data, an organization increases the likelihood that sensitive data will be exposed outside of the organization by either a malicious insider or a compromised system. Insider threat is one of the major issues facing organizations. Though some insiders do not have malicious intent, some scenarios create the perfect storm for the leaking of sensitive, personal data, especially health data. For example, in recent years, there have been several highly publicized events where individuals with celebrity status had their personal health information exposed by an insider of the health care organization. While these events are publicized, there are numerous others that are not. Friends, family members, co-workers or acquaintances access the personal health records of an individual outside of the organizations' policy, thereby violating that individual's right to privacy. To address this problem an organization must specify policies and employ mechanisms that limit an employee's access to data based on that which is needed to perform their daily tasks. For example, a lab tech may need information that identifies

[28] LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 23; Michael Daugherty March 4, 2014 Deposition Transcript, pp. 198-199.

the patient, but may not need the patient's insurance information. Additionally, when an organization has information about a large number of people, it is not only necessary to limit the types of information that an employee within a specific role may access, but it is also important to limit the number individuals whose Personal Information the employee may access. Doing so reduces the impact of a malicious insider.

82. In addition to the insider threat, when data may be accessed by multiple parties, the likelihood that the data may be accessed from a computer that has been compromised also increases. This is especially the case for organizations that do not have a comprehensive information security plan, and have security practices that are at best reactive. In such cases, when data is downloaded to a compromised computer, vulnerabilities on that computer may expose the data to individuals outside of the organization.

83. A multi-pronged, defense in depth, approach must be used to effectively restrict access to data. The organization must first define roles for its employees and specify the types of data that are needed to complete the tasks that have been assigned to those roles. To enforce these roles, IT practitioners have long used role-based access control mechanisms to restrict access to sensitive data resources. These mechanisms should be employed to restrict access to data files and to applications that mediate access to the data.

84. Based on my review of evidence from the record, I have formed the opinion that LabMD did not use adequate measures to prevent employees from accessing Personal Information that was not needed to perform their jobs.

a. Record evidence shows that LabMD is unable to specify the types of Personal Information that each of its employees was permitted to access via LabMD's network and can specify only that its employees had "various levels of access" to various types of

Personal Information and that "all employees could gain knowledge of any Personal Information regarding Consumers to the extent it was necessary to the performance of their job duties."[29]

b. Because LabMD cannot specify the types of Personal Information that each of its employees was permitted to access via LabMD's network, I conclude that LabMD did not specify policies and employ mechanisms to limit its employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs.

85. LabMD could have specified policies and implemented access control mechanisms to limit its employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs at relatively low cost. Operating systems and applications have access control mechanisms embedded in them. Therefore, correcting this issue would have required only the time of trained IT staff and could have been done at relatively low cost.

D. Information Security Training – Complaint ¶10(d)

86. Complaint Counsel has asked me to provide an opinion as to whether LabMD adequately trained employees to safeguard Personal Information. My opinion is organized as follows: (1) an explanation of the importance of training; and (2) my opinion, including some examples of key evidence supporting those opinions.

87. The user is the weakest link in any information security program. A flawless security mechanism can be rendered ineffective by an untrained user. For example, a username/password

[29] LabMD's February 20, 2014 and March 17, 2014 responses to Complaint Counsel's Interrogatory No. 2. See also, for example, March 10, 2014 Order on Complaint Counsel's Motion for Discovery Sanctions, p. 5.

authentication mechanism is only effective when users create strong passwords. Weak passwords that are short in length, contain dictionary words, contain the names of relatives, or favorite sports teams are more easily guessed than others. Therefore, an organization should train its employees on how to use any security mechanisms that require employee action or any security mechanisms that employees are not technically prevented from reconfiguring (such as disabling a firewall on a workstation without IT staff approval).

88. Employees also should receive periodic training on expected and acceptable use of computing facilities and current threats and best usage practices.

89. Since computer threats and vulnerabilities are always evolving, IT practitioners should receive periodic training on the most recent advances in protecting against such threats. Several nationally recognized organizations provide low-cost and free IT security training courses.[30]

90. I see no evidence in the record indicating that LabMD's non-IT employees received training on how to use security mechanisms or training on the consequences of reconfiguring security settings in applications and security mechanisms on their computers, such as enabling file-sharing, which I discuss in Section VIII.G, below.

91. Record evidence shows that LabMD did not adequately train employees to safeguard Personal Information or provide appropriate opportunities for its IT employees to receive formalized security related training about evolving threats and how to protect against them.[31] This resulted in gaps in their knowledge and a creation of security processes that were reactive, incomplete, ad hoc, and ineffective. For example, prior to 2010:

[30] For example, the Center for Information Security Awareness, formed in 2007, provides free security training for individuals and businesses with less than 25 employees. The SysAdmin Audit Network Security Institute (SANS) formed in 1989, provides free security training webcasts. Additional free training resources may be found at http://msisac.cisecurity.org/resources/videos/free-training.cfm. The Computer Emergency Response Team (CERT) at Carnegie Mellon University has e-learning courses for IT professionals for as low as $850.

[31] See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 52-53, 60-61.

a. Penetration testing was never done;[32]

b. Software with known flaws was not updated on servers that contained Personal Information;[33]

c. Firewalls were disabled on servers that contained Personal Information;[34]

d. Servers executed software that was no longer supported by vendors, including operating system and antivirus software;[35]

e. There was no uniform policy requiring strong passwords or expiration of passwords;[36]

f. Personal Information was transmitted and stored in an unencrypted format;[37]

g. At least some employees were given administrative access accounts and were able to download and install software without restriction, etc.[38]

92. LabMD could have adequately trained employees to safeguard Personal Information at relatively low cost.[39]

E. Use of Authentication Related Security Measures – Complaint ¶10(e)

93. Complaint Counsel has asked me to provide an opinion as to whether LabMD required employees, or other users with remote access to the network, to use common authentication-

[32] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 92, 281-282.

[33] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

[34] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 293-294.

[35] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 271-274; FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035).

[36] See, for example, Robert Hyer December 13, 2013 Deposition Transcript, pp. 25-27, 45-46; Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 153-154; John Boyle February 5, 2013 Investigational Hearing Transcript, pp. 181-184.

[37] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 62-64, 302-304.

[38] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 172; Alison Simmons Investigational Hearing Transcript, pp. 37-39; Robert Hyer December 13, 2013 Deposition Transcript, pp. 27-29.

[39] See, for example, footnote 30, above, and the accompanying text.

related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication. My opinion is organized as follows: (1) an explanation of why using authentication-related security measures is important; (2) a discussion of common authentication-related security measures to limit access; and (3) my opinion, including some examples of key evidence supporting those opinions.

94. Organizations should use strong authentication mechanisms to control access to workstations. Usernames/passwords are one such mechanism, but the effectiveness of this mechanism depends on the strength of the passwords and how the passwords are stored and managed. An organization should specify policies on how to create strong passwords. For example, password policies should specify acceptable length, required characters (numbers, case, symbols), lifetime, password history, passwords to avoid, etc. To enforce these policies: password management should be centralized; passwords should not be stored in clear text; and a cryptographic hash should be applied to the password before it is stored.

95. Based on my review of evidence from the record, I have formed the opinion that LabMD did not require employees or other users with remote access to its network, to use common, effective authentication-related security measures.

a. Record evidence shows that LabMD did not provide specific strong password policies or enforcement mechanisms to ensure that strong passwords were being used to authenticate users and authorize them to access LabMD's network, either on site or remotely. For example:

- LabMD billing employee Sandra Brown testified that she used the same username, sbrown, and password, labmd, to access her LabMD computer on site and remotely from 2006 to 2013.[40]

[40] See Sandra Brown January 11, 2014 Deposition Transcript, p. 13.

- LabMD created weak passwords for the nurses' user accounts that were created on the computers that it placed in its physician clients' offices. The typical password included the nurse's initials.[41]

- Although the Windows operating systems that LabMD used provided a centralized scheme to manage passwords, LabMD did not use that functionality.[42]

- Requiring two-factor authentication for remote users would have implemented a defense in depth strategy and could have compensated for LabMD's failure to require the use of strong passwords. LabMD did not use two-factor authentication.[43]

b. Record evidence shows that between at least October 2006 and June 2009, passwords required for access to Personal Information were shared by multiple LabMD employees.[44]

96. LabMD could have easily implemented strong authentication-related security measures at low cost.

F. Maintenance and Updating of Operating Systems– Complaint ¶10(f)

97. Complaint Counsel has asked me to provide an opinion as to whether LabMD maintained and updated operating systems of computers and other devices on its network. My opinion is organized as follows: (1) an explanation of the risks of using outdated software; and (2) my opinion, including some examples of key evidence supporting those opinions.

[41] See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 46-48; Letonya Randolph February 4, 2014 Deposition Transcript, pp. 39-41.

[42] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 171-172; Robert Hyer December 13, 2013 Deposition Transcript, pp. 84-88.

[43] See, for example, Alison Simmons, May 2, 2013 Investigational Hearing Transcript, pp. 47, 144, 152, 156; Curt Kaloustian May 3, 2013, Investigational Hearing Transcript, pp. 254-258; Matthew Bureau January 10, 2014 Deposition Transcript, pp. 83-84; Lawrence Hudson January 13, 2014 Deposition Transcript, pp. 74-75, 89, 183; Letonya Randolph February 4, 2014 Deposition Transcript, pp. 38-41.

[44] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 79; Robert Hyer December 13, 2013 Deposition Transcript, pp. 26-27, 45, 62, 74-75.

98. Researchers have found that experienced programmers introduce 1 bug per every 10 lines of code that they write.[45] Therefore, for a program like Windows Server 2003[46] that has 50 million lines of code, you can expect approximately 5 million software bugs to be introduced while the software is being developed. While many of the bugs will be detected and fixed during system testing, not all bugs will be identified before the product is shipped. In addition, code that was added to fix a problem may also introduce new bugs.

99. Hackers exploit software bugs to gain unauthorized access to computer resources and data. To limit these exploits, IT practitioners should connect to product notification systems and immediately apply remediation processes and updates for vulnerabilities that have been identified. These systems provided freely available notifications from vendors, CERT, OSVDB, NIST, and others throughout the Relevant Time Period.

100. Based on my review of evidence from the record, I have formed the opinion that through at least 2010, LabMD did not adequately maintain and update operating systems of computers and other devices on its network.

a. Record evidence shows that LabMD servers executed software that had vulnerabilities that had been identified and reported by the security and IT community several years prior to being detected on LabMD computers.[47] This time delay indicates that LabMD was neither knowledgeable of nor responsive to security alerts and software updates for the products that it used.

[45] See Humphrey, Watts, "A Discipline for Software Engineering," Addison-Wesley Professional 1995.

[46] LabMD used Windows Server 2003 on at least some of its servers in May 2010. See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

[47] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

b. Record evidence shows that LabMD did not apply software updates in accordance with the policies it claims were in place during the Relevant Time Period[48] and had no policy for updating the software on hardware devices such as firewalls and routers.

c. Record evidence shows that LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired by Microsoft.[49] The support life-cycle for Windows NT 4.0 ended on June 30, 2004, and Microsoft retired public and technical support and security updates on December 31, 2004. In a Microsoft press release, Microsoft states "Microsoft is retiring support for these products because the technology is outdated and can expose customers to security risks. The company recommends that customers who are still running Windows NT 4.0 begin migrations to newer, more secure Microsoft operating system products as soon as possible."[50]

d. Record evidence shoes that the LabMD Labnet server was running a version of Veritas Backup software that was configured with the default administrative password. This vulnerability had a Level 5 (Urgent Risk) rating, which means that an attacker can compromise the entire host. This problem was detected in 2010, and the corresponding solution was available as early as August 15, 2005. The Veritas software on the Labnet server also contained a Level 4 (Critical) buffer overflow vulnerability that would allow an attacker to execute arbitrary code on the remote host.[51] This problem was also detected

[48] See, for example, FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035); FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006); FTC-LABMD-003590 through FTC-LABMD-003621 (CX0007).

[49] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 271-274.

[50] "Q&A: Support for Windows NT Server 4.0 Nears End; Exchange Server 5.5 to Follow in One Year," https://www microsoft.com/en-us/news/features/2004/dec04/12-03ntsupport.aspx, last accessed March 17, 2014.

[51] Level 4 risks are "Vulnerabilities expose highly sensitive information and provide hackers with remote user capabilities. Intruders have partial access to file system; for example, full read access without full write access."

in 2010, and the corresponding solution was made available by the vendor on July 11, 2007.

e. Record evidence shows that several LabMD servers were running Integrated Information Services (IIS) web servers that used an insecure version of the Secure Socket Layer protocol (SSL 2.0).[52] This vulnerability had a Level 3 (High Risk) rating, which means that it provided hackers with access to specific information on the host, including security settings.[53] The vulnerability was detected on LabMD servers in 2010. Microsoft provided instructions on how to disable SSL 2.0 as early as April 23, 2007. Microsoft released Windows Server 2008 along with IIS 7.0 on February 27, 2008 and recommended both as upgrades to address the SSL 2.0 flaw. Thus, remediation for the flaw was available for three years prior to the vulnerability being detected on LabMD's network by the ProviDyn scan.

101. LabMD could have maintained and updated operating systems of computers and other devices on its network at relatively low cost.

G. Prevention and Detection of Unauthorized Access – Complaint ¶10(g)

102. Complaint Counsel has asked me to provide an opinion as to whether LabMD employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network. My opinion is organized as follows: (1) an explanation of the available measures and how they could have been deployed to prevent or detect unauthorized access to

[52] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070). SSL is the protocol that ensures that data is encrypted for https.

[53] Level 3 risks are "High Risk vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying)." FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

Personal Information; and (2) my opinion, including some examples of key evidence supporting those opinions.

103. Since security threats and vulnerabilities are changing constantly, security mechanisms that prevent an attack can never be exhaustive. Therefore, a defense in depth strategy must include mechanisms that attempt to prevent the exploitation of vulnerabilities by an attacker and detect unauthorized access when an attack is successful. The process of detection enables the organization to identify and patch holes in its security system.

104. There are several proactive, measures that should be employed, as part of a defense in depth strategy, to prevent the unauthorized sharing of Personal Information with external entities, including:

a. Employees should be given non-administrative accounts on workstations, thereby preventing them from installing software. Windows includes the functionality to enforce this policy in its operating systems package. This is a cost free measure.

b. Backups of Personal Information should be stored on devices that are isolated from other employee activities. An employee's workflow may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, unauthorized changes, etc. Therefore, backups of Personal Information should not be stored on multi-purpose employee workstations. Enforcing such a policy could be cost-free, if the organization designated an existing device for storage purposes only.

c. Windows operating systems provide the functionality to allow users to create folders that are stored on their individual workstations that can be shared with others.[54]

[54] These folders are different from shared folders on a network server that are centrally managed by IT staff.

When a folder is shared, it allows others to view the files that are contained within the folder.

d. While shared folders facilitate document sharing within an organization, there are many opportunities to mis-configure the sharing settings, which may lead to the inadvertent sharing of sensitive information with unauthorized parties. Such misconfigurations may include: giving read/write permissions to unauthorized parties, including restricted files in the shared folders, not including password protection, etc. In addition to the risk of misconfigurations, file-sharing applications, like LimeWire, also present the contents of shared folders to other users of those applications as information that is available to be downloaded. Therefore, employees should not be permitted to create shared folders on their workstations. Enforcing a no-shared folders policy requires no additional software, and can be achieved by configuring folder settings to disallow sharing and periodic monitoring of those settings.

e. A firewall should be employed at the network gateway to block all unwanted traffic from entering the network. The gateway firewall could be configured to block traffic destined to all unauthorized applications, such as file-sharing applications, which in turn would prevent traffic for those applications from entering the network. This type of configuring would create a list of acceptable applications and was routinely done by IT practitioners throughout the Relevant Time Period.

f. In addition, all employee workstations should be configured to use a software firewall. On August 25, 2004, Microsoft released its Windows Firewall as part of Windows XP Service Pack 2. This software firewall could be configured to block all incoming connection requests to a workstation. This would prevent, for example, users of file-sharing applications, like LimeWire, from establishing a successful connection with a workstation and downloading shared files. The Windows Firewall accompanied the operating system at no cost to the customer.

g. Properly configuring firewalls at the network gateway and on employee workstations implements a defense in depth strategy for network protection. This provides protection and the outer network layer and the inner workstation layer to provide more robust protection against unauthorized attempts to access the network infrastructure.

h. File Integrity Monitors (FIM) take an initial snapshot of the files that are stored on a computer and periodically monitor the system to determine whether any changes have occurred. Any change may indicate malicious activity and raises an alert notification, indicating further investigation is needed. A FIM can be used to determine the presence of unauthorized software on a system. There are both free and commercially available FIM products. Stealth[55] and OSSEC are examples of free products, and Tripwire is an example of a commercial product. These are the types of mechanisms that IT practitioners used regularly throughout the Relevant Time Period.

105. Based on my review of evidence from the record, I have formed the opinion that LabMD did not employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network.

a. Record evidence shows that LabMD actively stored backups of highly sensitive Personal Information on the Billing Manager's workstation.[56] At least one document

[55] "Center for Information Technology, University of Groningen -- SSH-based Trust Enforcement Acquired through a Locally Trusted Host," http://stealth.sourceforge.net/, accessed on March 17, 2014.

[56] See FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006).

containing [a backup of] Personal Information was stored in a shared folder on the Billing Manager's workstation, which made it accessible to the unauthorized file-sharing application that had been previously installed on that computer.

b. As discussed in Paragraph 61, above, record evidence shows that LabMD did not detect and remove the file-sharing application, LimeWire, until 2008, two to three years after it had been installed.[57] Had LabMD used FIM products to periodically monitor the Billing Manager workstation during this two to three year period, it might have detected the LimeWire application by, for example, detecting its installation or detecting music files downloaded through LimeWire. FIM therefore would have strengthened a defense in depth approach.

c. Record evidence shows that LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network.[58]

106. LabMD could have employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network at relatively low cost.

[57] See, for example, July 16, 2010 Letter from P. Ellis to A. Sheer (FTC-LABMD-002495 through FTC-LABMD-002503).

[58] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 98-103.

IX. Conclusion

107. Based on my review of the materials described in Section VI, above, my experience described in Section II, above, and the specific opinions presented in Section VIII, above, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network throughout the Relevant Time Period of January 2005 through July 2010, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures.

Dated: March 18, 2014

Raquel Hill, Ph.D.

Appendix A

Home Address:
734 E. Moss Creek
Drive
Bloomington, IN 47401
Phone(217)369-0105
hill raquel@gmail.com

School of Informatics and
Computing
Indiana University
Bloomington, IN 47405
Phone (812) 856-5807
E-mail
ralhill@indiana.edu
www.cs.indiana.edu/~ral
hill

Raquel Hill

Education

University of Illinois Urbana, IL

August 2003- July 2005 Post Doctoral Research Associate

Harvard University Cambridge, MA

November 2002 PhD Computer Science

- Dissertation: Sticky QoS: A Scalable Framework for Resource Reservations.
- Advisor: H.T. Kung

Georgia Institute of Technology Atlanta, GA

March 1993 MS Computer Science

June 1991 BS Computer Science with Honors

Professional Experience

Harvard University, Cambridge, MA, **Visiting Scholar,** School of Engineering and Applied Science, **Center for Research on Computation and Society,** 9/2013 – 5/2014

Indiana University, Bloomington, Indiana, **Associate Professor,** School of Informatics and Computing, 6/2012 –Present

Indiana University, Bloomington, Indiana, **Assistant Professor,** School of Informatics and Computing, 08-2005 – 6/2012

Indiana University, Bloomington, Indiana, **Research Fellow, Kinsey Institute,** 12/2010 – Present

Jackson State University, Jackson, Mississippi, **Adjunct Professor, Department of Computer Science,** 2010- Present

University of Illinois, Urbana, Illinois, **Post-Doctoral Research Associate,** Joint Appointment with Department of Computer Science and NCSA, 08/2003 – 07/2005

Georgia Institute of Technology Atlanta, GA, **Lecturer,** within the School Electrical and Computer Engineering, 11/2002 – 08/2003

Professional Experience

Harvard University, Cambridge, MA, **Research Assistant** 09/1998 – 09/2002

IBM Research , Hawthorne, NY, **Intern**, Summer 1999

Digital Equipment Corporation, Cambridge, MA, **Intern**, Summer 1997

Nortel Networks , RTP, NC, **Member of Scientific Staff**, 08/1993 – 08/1996

Hayes MicroComputer Products, Atlanta, GA, **Coop Student**, 03/1993-07/1993

Cray Research, Eagan, MA, **Intern**, Summer 1992

Cray Research, Chippewa Falls, WI, **Intern**, Summer 1991

IBM Corporation, Atlanta, GA, **Co-op Student**, 06/1987-9/1990

Grants

IBM Corporation, Equipment Grant – Cryptographic Co-processors
Equipment Value: $75,000.00 Date: 9/01/05 – Present

CACR: Privacy Enhanced Online Human Subjects Data Collection
Total Award Amount: $49,999.99 Date: 07/01/09 – 12/31/10
Role: PI Source of Support: IU

TC: Large: Collaborative Research: Anonymizing Textual Data and Its Impact on Utility
Total Award: $568,895 Date: 9/01/10 – 8/31/14
Role: PI Source of Support: NSF

FRSP: Childhood Obesity Studies with Secure Cloud Computing
Total Award: $36,500 Date: 9/1/11 – 12/31/13
Role: PI

Publications

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J. R. Heiman, L. Xiong, Evaluating Utility: Towards an Understanding of Sharing Differentially Private Behavioral Science Data, (Under Review).

Raquel Hill, Michael Hansen, Veer Singh, "Quantifying and Classifying Covert Channels on Android", *Journal of Mobile Networks and Applications*, Springer US, DOI. 10.1007/s11036-013-0482-7, (November 2013).

Publications

D. Hassan, R. Hill, "A Language-based Security Approach for Securing Map-Reduce Computations in the Cloud", To appear in the *Proceedings of the 6th IEEE/ACM International Conference on Utility and Cloud Computing*, December 9-12, 2013, Dresden, Germany.

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J.R. Heiman, L. Xiong, "An Empirical Analysis of a Differentially Private Social Science Dataset" In the *Proceedings of PETools: Workshop on Privacy Enhancing Tools, Held in Conjunction with the Privacy Enhancing Tools Symposium*, July 9, 2013, Bloomington, IN.

M. Hansen, R. Hill, S. Wimberly, Detecting Covert Communications on Android. In the *Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN 2012)*, October 22-25, 2012, Clearwater, Florida.

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, J. Heiman, Uniqueness and How it Impacts Privacy in Health-Related Social Science Datasets, In the Proceedings of the *ACM International Health Informatics Symposium (IHI 2012)*, January 28-30, 2012, Miami Florida.

J. Harris, R. Hill, Static Trust: A Practical Framework for Trusted Networked Devices, In the *Proceedings of 44th Hawaii International Conference on System Sciences, Information Security and Cyber Crime Track*, (Kauai, HI, 2011), 10 pages, CDROM, IEEE Computer Society.

Al-Muhtadi, Raquel Hill and Sumayah AlRwais "Access Control using Threshold Cryptography for Ubiquitous Computing Environments". *Journal of King Saud University Computer and Information Sciences*, No. 2, Vol. 23, (July 2011).

R. Hill, J. Al-Muhtadi, W. Byrd, An Access Control Architecture for Distributing Trust in Pervasive Computing Environments, at the *6th IEEE/IFIP Symposium on Trusted Computing and Communications (TrustCom)*, In the *Proceedings of 8th IEEE/IFIP Conference on Embedded and Ubiquitous Computing*, (Hong Kong, China, 2010), 695-702.

J. Harris, R. Hill, Building a Trusted Image for Embedded Communications Systems, In the *Proceedings of 6th Annual Cyber Security and Information Intelligence Workshop*, (Oakridge, TN, 2010), ACM, NY, 65:4.

L. Wang, R. Hill, Trust Model for Open Resource Control Architecture, at *3rd IEEE International Symposium on Trust, Security and Privacy for Emerging Applications*, In the *Proceedings of 10th IEEE International Conference on Computer and Information Technology*, (Bradford, UK, 2010) 817-823.

Publications

Gilbert, J.E., MacDonald, J., Hill, R., Sanders, D., Mkpong-Ruffin, I., Cross, E.V., Rouse, K., McClendon, J., & Rogers, G. (2009) Prime III: Defense-in-Depth Approach to Electronic Voting. In the *Journal of Information Security and Privacy*, 2009

J. Al-Muhtadi, R. Hill, R. Campbell, D. Mickunas, Context and Location-Aware Encryption for Pervasive Computing Environments, In *Proceedings of the 4th IEEE Conference on Security in Pervasive Computing and Communications Workshops*, (Pisa, Italy, 2006), 283-289.

R. Hill, S. Myagmar, R. Campbell, Threat Analysis of GNU Software Radio, In the *Proceedings of the 6th World Wireless Congress*, (San Francisco, CA, 2005).

A. Lee, J. Boyer, C. Drexelius, P. Naldurg, R. Hill, R. Campbell, Supporting Dynamically Changing Authorizations in Pervasive Communication Systems, In the *Proceedings of the 2nd International Conference on Security in Pervasive Computing*, (Boppard, Germany, 2005), 134-150.

R. Hill, G. Sampemane, A. Ranganathan, R. Campbell, Towards a Framework for Automatically Satisfying Security Requirements, In the *Proceedings of Workshop on Specification and Automated Processing of Security Requirements in conjunction with the 19th IEEE International Conference on Automated Software Engineering*, (Linz Austria, 2004), 179-191.

R. Hill, J. Al-Muhtadi, R. Campbell, A. Kapadia, P. Naldurg, A. Ranganathan, A Middleware Architecture for Securing Ubiquitous Computing Cyber Infrastructures, *5th ACM/IFIP/USENIX International Middleware Conference*, October 2004, *in IEEE Distributed Systems Online*, 5,9 (September 2004), 1-.

R. Hill, H.T. Kung, A Diff-Serv enhanced Admission Control Scheme, In *Proceedings IEEE Global Telecommunications Conference*, (San Antonio, TX, 2001), 2549-2555.

Refereed Abstracts

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, Privacy and De-Identification in High Dimensional Social Science Data Sets, *in the Proceedings of the 32nd Annual IEEE Symposium on Security and Privacy*, Oakland, California, May 22-25, 2011.

R. Hill, J. Camp, Communicating Risk within the GENI Infrastructure, *Workshop on GENI and Security*, University California, Davis, January 22-23, 2009.

R. Hill, J. Wang, K. Nahrstedt, Towards a Framework for Quantifying Non-Functional Requirements, *Grace Hopper Celebration of Women in Computing*, October 2004.

Refereed Abstracts

J. Al-Muhtadi, R. Hill, R. Campbell, A Privacy Preserving Overlay for Active Spaces, *Ubicomp Privacy Workshop in conjunction with the Sixth International Conference on Ubiquitous Computing*, Nottingham, England, September 2004.

Posters

R. Hill, A.C. Solomon, E. Janssen, S. Sanders, J. Heiman, Privacy and Uniqueness in High Dimensional Social Science and Sex Research Datasets, Presented at the 37th Annual Meeting of the International Academy of Sex Research, August 10-13, 2011, Los Angeles, California.

C. Boston, R. Hill, L. Moore, The Feasibility of Designing a Secure System to Prevent Surgical Errors Using RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

S. Camara, R. Hill, L. Moore, Understanding How RFID Technology Impacts Patient Privacy, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

R. Johnson, R. Hill, L. Moore, Evaluating and Mitigating the Security Vulnerabilities of RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

R. Hill, J. Wang, K. Nahrstedt, Quantifying Non-Functional Requirements: A Process Oriented Approach, *in the Proceedings of the 12th IEEE International Requirements Engineering Conference*, Kyoto, Japan, September 2004.

Technical Reports

R. Hill, J. Al-Muhtadi, Building a Trusted Location Service for Pervasive Computing Environments, Technical Report, TR646, Computer Science, Indiana University, 2007.

Dissertation

R. Hill, Sticky QoS: A Scalable Framework for Resource Reservations, Doctoral Dissertation in Computer Science, Harvard University Division of Engineering and Applied Sciences, November 2002.

Symposiums

"Protecting Privacy in Sex Research: Challenges and solutions offered by new technologies and recommendations for the collection, protection and the sharing of multi-dimensional data", **Speakers:** Raquel Hill, School of Informatics and Computing, Indiana University, Ulf-Dietrich Reips, iScience, University of Deusto, Bilbao, Spain, Stephanie Sanders, Gender Studies, Indiana University, The 38th Annual Meeting of the International Academy of Sex Research, July 8-12, 2012, Lisbon, Portugal

Invited Talks

"Understanding the Risk of Re-Identification in Behavioral Science Data", Technology in Government Topics in Privacy Seminar, Data Privacy Lab, Harvard University, Cambridge, MA, November 4, 2013.

Invited Talks

"Evaluating the Utility of a Differentially Private Behavioral Science Dataset", Center for Research on Computation and Society (CRCS), Harvard University, Cambridge, MA, October 2, 2013.

"Balancing the Interests in Developing and Sharing Behavioral Science Data", Workshop on Integrating Approaches to Privacy Across the Research Lifecycle, Harvard University, Cambridge, MA, September 24-25, 2013.

"Kinsey Goes Digital", Kinsey Institute's Board of Trustees Meeting, Indiana University, Bloomington, IN, May 20, 2011.

"Integrity-Based Trust for Networked Communications Systems", Center for Applied Cyber-security Research, Indiana University, Bloomington, IN, December 2, 2010.

"From Kinsey to Anonymization: Approaches to Preserving the Privacy of Survey Participants", Department of Mathematics and Computer Science, Emory University, Atlanta, GA, November 19, 2010; Indiana University, Bloomington, IN, November 12,2010.

"PlugNPlay Trust for Embedded Communications Systems", Purdue University, CERIAS, October 14, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

"Characterizing Trustworthy Behavior of Email Servers", CAARMS 2009, Rice University, June 23-26, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

"Hardware Enabled Access Control for Electronic Voting Systems", Rose Hulman, January 6, 2009; Jackson State University, February 26, 2009

"Hardware-enabled Access Control for the Prime III Voting System", Auburn University, June 16, 2008

"Understanding the Behaviors of Malicious Users of Pervasive Computing Environments", ARO/FSTC Workshop on Insider Attacks and Cyber Security, June 11-12, 2007, Arlington, Virginia.

"Trusting Your Security", Second Annual Network Security Workshop, Lehigh University, May 15-16, 2006

"Establishing a Trusted Computing Base for Software Defined Radio", Information Security Institute, Johns Hopkins University, February 2005, Baltimore, Maryland.

Invited Talks

"Towards a Framework for Automatically Satisfying Security Requirements", Department of Computer Science, Queens University, October 2004, Kingston, Ontario, Canada.

"Overlay QoS", Department of Computer Science, Auburn University, February 2004, Auburn, Alabama.
"Distributed Admissions Control for Sticky QoS", *Ninth Annual Conference for African-American Researchers in the Mathematical Sciences,* June 2003, West LaFayette, Indiana.

"Distributed Admissions Control for Sticky QoS". *Sixth Informs Telecommunications Conference,* March, 2002, Boca Raton, Florida.
Former Congressman Lee Hamilton, Professor Fred Cate, and Professor Raquel Hill, "Security and Privacy in a Cyberwar World: A conversation about Edward Snowden, the NSA and the outlook for reform", *Indiana Statewide IT Conference*, Indiana University, Bloomington, IN October, 29, 2013

Panels

R. Hill, "Building Trusting Systems; Trusting Your Security", *Workshop on Useable Security, co-located with 11th Conference on Financial Cryptography and Data Security,* February 2007, Lowlands, Scarborough, Trinidad/Tobago.

R. Hill, R. Campbell, "Understanding, Managing and Securing Ubiquitous Computing Environments", *Grace Hopper Celebration of Women in Computing*, October 2004, Chicago, Illinois.

C. Lester, R. Hill, M. Spencer, "Making Waves: Navigating the Transition from Graduate Student to Faculty Member", *Grace Hopper Celebration of Women in Computing*, San Diego, California, Oct. 4-6, 2006.

Teaching

University	Course	Semesters Taught
Indiana University	I230 Analytical Foundations of Security	Spring 2006, Fall 2007-2011
	CSCI P438 Introduction to Computer Networks	Fall 2009,2010,2012
	CSCI H343 Data Structures (Honors	Fall 2011,2012
	CSCI B649 Trusted Computing	Spring 2006-2011
	CSCI B649 Data Protection	Spring 2013
Georgia Institute of Technology	ECE 2030 Introduction to Computer Engineering	Spring 2003, Summer 2003

Professional Activities

Member of Technical Program Committee

- IEEE International Conference on Information Technology (ITCC) 2005, Pervasive Computing Track
- IEEE International Conference on Communications 2006: Network Security and Information Assurance Symposium
- Indiana Women in Computing Conference February 2006
- Workshop on Security, Privacy and Trust for Pervasive Computing Applications, September 2006, 2007, 2008, 2009, 2010
- Middleware Support for Pervasive Computing Workshop (PERWARE) at the 4th Conference on Pervasive Computing and Communications, March 2007, 2008, 2009
- IEEE International Conference on Computer Communications and Networks, (ICCCN'06), Network Security and Dependability Track, October 2006; (ICCCN'07), Pervasive Computing and Mobile Networking Track, August 2007.
- IFIP Sixth International Conference on Networking (Networking 2007, 2008),
- Fourth International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, March 17-20, 2008 (Tridentcom 2008)
- First International ICST Conference on Mobile Wireless Middleware, Operating Systems and Applications, February 13-15, 2008, (Mobileware 2008, 2009,2010

Member of Review Panel

- **National Science Foundation**
- **Department of Energy**

Appendix B

Appendix B
Materials Considered or Relied Upon

IH Transcripts and Exhibits	**Bates Range**
13.02.05 Boyle, John - Transcript	FTC-000001-FTC-000115
13.02.05 Boyle, John - Exhibits	FTC-000116-FTC-000376
13.02.06 Daugherty, Michael - Transcript	FTC-000377-FTC-000416
13.02.06 Daugherty, Michael - Exhibit #8	FTC-000225-FTC-000246
13.02.06 Daugherty, Michael - Exhibit #14	FTC-000283-FTC-000304
13.02.06 Daugherty, Michael - Exhibit #23	FTC-000417-FTC-000423
13.05.02 Simmons, Alison - Transcript	FTC-000424-FTC-000493
13.05.02 Simmons, Alison - Exhibits	FTC-000494-FTC-000512
13.05.03 Kaloustian, Curt - Transcript	FTC-000513-FTC-000638
13.05.03 Kaloustian, Curt - Exhibits	FTC-000639-FTC-000656

Deposition Transcripts and Exhibits

14.01.09 Maire, Chris
14.01.10 Bureau, Matt
14.01.11 Brown, Sandra
14.01.13 Hudson, Lawrence
14.01.17 Maxey, Jerry Southeast Urology Network Rule 3.33
14.01.24 Howard, Patrick
14.04.28 Boyle, John
14.02.04 Randolph, Letonya Midtown Urology Rule 3.33
14.02.05 Simmons, Alison
14.02.06 Martin, Jeff
14.02.07 Gilbreth, Patricia
14.02.14 Bradley, Brandon
14.02.17 Carmichael, Lou
14.03.04 Daugherty, Michael LabMD Rule 3.33
14.02.10 Daugherty, Michael
14.01.25 Garrett, Karalyn
14.02.21 Harris, Nicotra
14.02.11 Parr, Jennifer
14.01.31 Sandrev, Peter Cypress Communication Rule 3.33
14.02.27 Truett, Allen
13.12.02 Dooley, Jeremy
13.11.21 Boback, Robert Tiversa Rule 3.33
13.12.13 Hyer, Robert

Correspondence	**Bates Range**
10.02.24 Ellis Letter	FTC-LABMD-002506-FTC-LABMD-002520
10.06.04 Ellis Letter	FTC-LABMD-002523-FTC-LABMD-002524
10.07.16 Ellis Letter	FTC-LABMD-002495-FTC-LABMD-002503
10.07.16 Ellis Exhibits	FTC-LABMD-002505-FTC-LABMD-003131

10.08.30 Ellis Letter	FTC-LABMD-003132-FTC-LABMD-003137
10.08.30 Ellis Exhibits	FTC-LABMD-003138-FTC-LABMD-003270
11.05.16 Rosenfeld Letter	FTC-LABMD-003445-FTC-LABMD-003452
11.05.16 Rosenfeld Exhibits	FTC-LABMD-003453-FTC-LABMD-003628
11.05.31 Rosenfeld Letter	FTC-LABMD-003629-FTC-LABMD-003634
11.05.31 Rosenfeld Exhibits	FTC-LABMD-003635-FTC-LABMD-003748
11.07.22 Rosenfeld Email	FTC-LABMD-003749-FTC-LABMD-003750
11.07.22 Rosenfeld Email	FTC-LABMD-003756-FTC-LABMD-003756
11.07.22 Rosenfeld Email-Screenshots	FTC-LABMD-003757-FTC-LABMD-003761
11.12.21 CID to Daugherty and Responses	FTC-000417-FTC-000423
13.01.17 CID to Daugherty and Responses	NA
11.12.21 CID to LabMD and Responses	FTC-000116-FTC-000127
13.01.17 CID to LabMD and Reponses	NA

Documents Produced by LabMD

FTC-LABMD-000001-FTC-LABMD-000304
FTC-LABMD-000306-FTC-LABMD-000385
FTC-LABMD-000388-FTC-LABMD-000603
FTC-LABMD-000605-FTC-LABMD-000634
FTC-LABMD-000636-FTC-LABMD-000646
FTC-LABMD-000648-FTC-LABMD-000776
FTC-LABMD-003139-FTC-LABMD-003444
FTC-LABMD-003453-FTC-LABMD-003628
FTC-LABMD-003635-FTC-LABMD-003748
FTC-LABMD-003752-FTC-LABMD-003761
FTC-LABMD-003763-FTC-LABMD-004358
FTC-LABMD-004514-FTC-LABMD-004536
FTC-LABMD-004576-FTC-LABMD-004677
FTC-LABMD-004782-FTC-LABMD-004851
FTC-LABMD-004882-FTC-LABMD-004891
FTC-LABMD-004897-FTC-LABMD-004906
FTC-LABMD-004922-FTC-LABMD-004950
FTC-LABMD-004975-FTC-LABMD-005129
FTC-LABMD-005160-FTC-LABMD-005221
FTC-LABMD-005250-FTC-LABMD-005310
FTC-LABMD-005644-FTC-LABMD-005651
FTC-LABMD-005686-FTC-LABMD-006637
FTC-LABMD-006820-FTC-LABMD-006823
FTC-LABMD-006828-FTC-LABMD-006835
FTC-LABMD-007128-FTC-LABMD-007132
FTC-LABMD-007212-FTC-LABMD-007342
FTC-LABMD-007463-FTC-LABMD-007507
FTC-LABMD-007619-FTC-LABMD-007627
FTC-LABMD-007636-FTC-LABMD-007659
FTC-LABMD-007990-FTC-LABMD-007994
FTC-LABMD-008022-FTC-LABMD-008036

FTC-LABMD-008108-FTC-LABMD-008124
FTC-LABMD-008780-FTC-LABMD-008783
FTC-LABMD-009955-FTC-LABMD-009958
FTC-LABMD-009960-FTC-LABMD-010060
FTC-LABMD-010513-FTC-LABMD-010615
FTC-LABMD-010654-FTC-LABMD-010660
FTC-LABMD-011103-FTC-LABMD-011106
FTC-LABMD-011116-FTC-LABMD-011120
FTC-LABMD-011855-FTC-LABMD-011858
FTC-LABMD-012751-FTC-LABMD-012755
FTC-LABMD-013286-FTC-LABMD-013289
FTC-LABMD-013304-FTC-LABMD-013308
FTC-LABMD-013441-FTC-LABMD-013448
FTC-LABMD-014422-FTC-LABMD-014483
FTC-LABMD-014512-FTC-LABMD-014521
FTC-LABMD-014533-FTC-LABMD-014607
FTC-LABMD-014613-FTC-LABMD-014620
FTC-LABMD-014625-FTC-LABMD-014680
FTC-LABMD-014689-FTC-LABMD-014692
FTC-LABMD-014699-FTC-LABMD-014869
FTC-LABMD-014896-FTC-LABMD-014952
FTC-LABMD-014957-FTC-LABMD-015016
FTC-LABMD-015020-FTC-LABMD-015218
FTC-LABMD-015242-FTC-LABMD-015245
FTC-LABMD-015414-FTC-LABMD-015430
FTC-LABMD-015457-FTC-LABMD-015477
FTC-LABMD-015491-FTC-LABMD-015525
FTC-LABMD-015542-FTC-LABMD-015962
FTC-LABMD-015994-FTC-LABMD-016063
FTC-LABMD-016135-FTC-LABMD-016141
FTC-LABMD-016148-FTC-LABMD-016179

Documents Produced by Tiversa
TIVERSA-FTC RESPONSE-000001-006904

Documents Produced by Sacramento Police Department
FTC-SAC-000001-FTC-LABMD-000044

Documents Produced by the Privacy Institute
FTC-PRI-000001-FTC-PRI-001719

Documents Produced by Cypress Communication, LLC
FTC-CYP-000001-FTC-CYP-000001
FTC-CYP-0001656-FTC-CYP-0001725
FTC-CYP-0001729-FTC-CYP-0001733
FTC-CYP-0001735-FTC-CYP-0001757

FTC-CYP-0001759-FTC-CYP-0001763
FTC-CYP-0001765-FTC-CYP-0001772
FTC-CYP-0001784-FTC-CYP-0001811
FTC-CYP-0001881-FTC-CYP-0001896
FTC-CYP-0001898-FTC-CYP-0001899
FTC-CYP-0001954-FTC-CYP-0001968
FTC-CYP-0001973-FTC-CYP-0001976
FTC-CYP-0001983-FTC-CYP-0001984
FTC-CYP-0002008-FTC-CYP-0002009
FTC-CYP-0002109-FTC-CYP-0002109

Documents Produced by ProviDyn, Inc.
FTC-PVD-000001-FTC-PVD-001582

Documents Produced by TrendMicro
FTC-TRM-000001-FTC-TRM-000455

Web Content Considered or Relied Upon

- The Center for Information Security Awareness, http://www.cfisa.org/, last accessed March 18, 2014.
- Center for Information Technology, University of Groningen -- SSH-based Trust Enforcement Acquired through a Locally Trusted Host, http://stealth.sourceforge.net/, last accessed March 16, 2014.
- The Computer Emergency Response Team (CERT), https://www.cert.org/, last accessed March 18, 2014.
- The Computer Emergency Response Team (CERT) -- Anonymous FTP Activity (1997), http://www.cert.org/historical/advisories/CA-1993-10.cfm, last accessed March 18, 2014.
- Cisco -- Cisco 1841 Integrated Services Router, http://www.cisco.com/c/en/us/products/routers/1841-integrated-services-router-isr/index.html, last accessed March 16, 2014.
- Common Vulnerabilities and Exposures – The Standard for Information Security Vulnerability Names, http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0527, last accessed March 16, 2014.
- Federal Communications Commission -- Cybersecurity for Small Businesses, http://www.fcc.gov/cyberforsmallbiz, last accessed March 16, 2014.
- Microsoft Forum -- Disable SSL v2 in IIS6?, http://forums.iis.net/t/1131343.aspx, last accessed March 16, 2014.
- Microsoft News Center -- Microsoft Windows Server 2003 Is Available Worldwide Today (April 24, 2003), http://www.microsoft.com/en-us/news/press/2003/apr03/04-24windowsserver2003launchpr.aspx, last accessed March 16, 2014.
- Microsoft Security TechCenter – Microsoft Security Bulletin MS05-019 – Critical, http://technet.microsoft.com/en-us/security/bulletin/ms05-019, last accessed March 16, 2014.
- Microsoft Security TechCenter – Security Guidance for IIS, http://technet.microsoft.com/en-us/library/dd450371.aspx, last accessed March 16, 2014.

- Microsoft Security TechCenter – Microsoft Security Advisory (2661254), http://technet.microsoft.com/en-us/security/advisory/2661254, last accessed March 16, 2014.
- Microsoft Security TechCenter – Microsoft Security Bulletin MS05-019 – Critical, http://technet.microsoft.com/en-us/security/bulletin/ms05-019, last accessed March 16, 2014.
- Microsoft Support – How to disable simple file sharing and how to set permissions on a shared folder in Windows XP, http://support.microsoft.com/kb/307874, last accessed March 16, 2014.
- Microsoft Support, http://support.microsoft.com/?id=187498, last accessed March 16, 2014.
- Microsoft Support – How to install and use the IIS Lockdown Wizard, http://support.microsoft.com/kb/325864, last accessed March 16, 2014.
- Microsoft Support – Microsoft Security Advisory: Update for minimum certificate key length, http://support.microsoft.com/kb/2661254, last accessed March 16, 2014.
- Microsoft Support, http://support.microsoft.com/kb/2661254, last accessed March 16, 2014.
- Multi-State Information Sharing & Analysis Center – Cyber Security Awareness Free Training and Webcasts, http://msisac.cisecurity.org/resources/videos/free-training.cfm, last accessed March 18, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2611, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2005-0048&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3509, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2002-1717&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2005-0048&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5969, last accessed March 16, 2014.

- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1491, Last accessed March 16, 2014.
- Nmap.org – www.nmap.org, last accessed March 18, 2014.
- Open Source SECurity, http://www.ossec.net/, last accessed March 16, 2014.
- Open Source Vulnerability DataBase, http://osvdb.org/76, last accessed March 16, 2014.
- Open Source Vulnerability DataBase, http://osvdb.org/show/osvdb/193, last accessed March 16, 2014.
- Symantec - Symantec Backup Exec for Windows Server: PRC Interface Heap Overflow, Denial of Service, http://securityresponse.symantec.com/avcenter/security/Content/2007.07.11a.html, last accessed March 17, 2014.
- Symantec – VERITAS Backup Exec for Windows Servers, VERITAS Backup Exec for NetWare Servers, and NetBackup for NetWare Media Server Option Remote Agent Authentication Vulnerability, http://securityresponse.symantec.com/avcenter/security/Content/2005.08.12b.html, last accessed March 17, 2014.
- The SysAdmin Audit Network Security Institute (SANS) – Information Security Resources, http://www.sans.org/security-resources/, last accessed March 18, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/us/archive/grayware/crck_vista.b, last accessed March 16, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/Malware.aspx?id=35451&name=CRCK_KEYGEN&language=au, last accessed March 16, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/us/archive/grayware/CRCK_KEYGEN.AU, last accessed March 16, 2014.
- U.S. Department of Health and Human Services – Health Information Privacy: The Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/, last Accessed March 18, 2014.

Articles & Publications

- Espenschied, Jon, "Five free pen-testing tools" (May 27, 2008), http://www.computerworld.com/s/article/9087439/Five_free_pen_testing_tools, last accessed March 16, 2014.
- Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, last accessed March 16, 2014.
- Halamka, John D., Szolovits, Peter, Rind, David, Safran, Charles, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information" Journal of the American Medical Informatics, (Nov-Dec 1997), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC61263/, last accessed March 16, 2014.

- Houston, Peter, "Q&A: Support for Windows NT Server 4.0 Nears End; Exchange Server 5.5 to Follow in One Year," https://www.microsoft.com/en-us/news/features/2004/dec04/12-03ntsupport.aspx, last accessed March 17, 2014.
- Kelly, Allen, "Proper Management of SSL Certificates: Why it is Critical to Your Organization - Part II" (September 8, 2011), http://www.symantec.com/connect/blogs/proper-management-ssl-certificates-why-it-critical-your-organization-part-ii, last accessed March 16, 2014.
- Kissel, Richard, "Small Business Information Security: The Fundamentals" (October 2009), http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf, last accessed March 16, 2014.
- NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments" (September 18, 2012), http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf, last accessed March 18, 2014.
- PCI Security Standards Council "PCI Technical and Operational Requirements for Approved Scanning Vendors, Version 1.1" (September 2006), https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf, last accessed March 18, 2014.
- SANS Institute_InfoSec Reading Room, "Understanding IIS Vulnerabilities - Fix Them!" (2001), http://www.sans.org/reading-room/whitepapers/webservers/understanding-iis-vulnerabilities-fix-them-296, last accessed March 16, 2014.
- SANS Institute_InfoSec Reading Room, "Cryptanalysis of RSA: A Survey" (2003), http://www.sans.org/reading-room/whitepapers/webservers/understanding-iis-vulnerabilities-fix-them-296, last accessed March 16, 2014.
- SANS Institute InfoSec Reading Room, "The Many Facets of an Information Security Program" (2003), https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343, last accessed March 18, 2014.
- Stoneburner, Gary, Goguen, Alice, Feringa, Alexis, "NIST Risk Management Guide for Information Technology Systems" NIST (July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, last accessed March 18, 2014.
- U.S. Department of Health and Human Services, HIPAA Security Series, "6 Basics of Security Risk Analysis and Risk Management" (March 2007), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf, last accessed March 18, 2014.
- Wagner, David, Schneier, Bruce, "Analysis of the SSL 3.0 protocol," https://www.schneier.com/paper-ssl.pdf, last accessed March 16, 2014.
- Woody, Carol, Clinton, Larry, Internet Security Alliance, "Common Sense Guide to Cyber Security for Small Businesses" (March 2004), http://isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf, last accessed March 18, 2014.

Books

- Humphrey, Watts, "A Discipline for Software Engineering," Addison-Wesley Professional (1995).

- National Research Council, "For the Record: Protecting Electronic Health Information" Washington, DC: The National Academies Press (1997), http://www.nap.edu/openbook.php?record_id=5595&page=R1, last accessed March 16, 2014.

FTC Provided Documents

- 13.08.28 Complaint
- 14.02.19 Complaint Counsel's Requests for Admission to Respondent LabMD
- 14.02.20 Revised Answer to Complaint Counsel's Interrogatory 1 and 2
- 14.03.03 Respondent's Objections and Responses to Complaint Counsel's Requests for Admission
- 14.03.10 Order Granting In Part and Denying In Part Complaint Counsel's Motion for Discovery Sanctions
- 14.03.14 Order on Complaint Counsel's Motion for Discovery Responses
- 14.03.17 Respondent's Supplemental Response to Complaint Counsel's First Set of Interrogatories

Miscellaneous

- Federal Register, Department of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information" (October 15, 2002), http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt, last accessed March 18, 2014.
- Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security_Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, last accessed March 16, 2014.

EXHIBIT 6

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Bureau of Consumer Protection
Division of Privacy and Identity Protection

January 27, 2014

VIA EMAIL AND COURIER

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

Re: In the Matter of LabMD, Inc., FTC Docket No. 9357

Dear Mr. Sherman:

This letter follows my letter of January 24, 2014. Enclosed is a disc containing Complaint Counsel's first production of documents responsive to LabMD, Inc.'s written discovery requests.

Specifically, the documents that appear at FTC-000894 through FTC-010652 are responsive to LabMD's Request for Production 10. The documents that appear at FTC-000894 through 002693 are responsive to LabMD's Interrogatory 18.

We will supplement this production with our continuing, rolling production of responsive, discoverable, non-privileged documents.

Please notify me when you have received the enclosed disc and I will then send you the encryption key.

Sincerely,

Laura Riposo VanDruff

Enclosure (1)

cc: Reed D. Rubinstein (*via* email)
Michael D. Pepson (*via* email)
Lorinda B. Harris (*via* email)
Hallee K. Morgan (*via* email)
Kent Huntington (*via* email)

Sunni Harris (*via* email)
Robyn Burrows (*via* email)

EXHIBIT 7

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Bureau of Consumer Protection
Division of Privacy and Identity Protection

March 3, 2014

VIA EMAIL AND COURIER

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

Re: In the Matter of LabMD, Inc., FTC Docket No. 9357

Dear Mr. Sherman:

This letter follows my letters of January 24, 2014, January 27, 2014, and February 19, 2014. Enclosed is a disc containing Complaint Counsel's third production of documents responsive to LabMD, Inc.'s written discovery requests.

Specifically, the documents that appear at FTC-013803 to FTC-013853 are responsive to Request for Production 4 and Interrogatory 11. The documents that appear at FTC-012347 to FTC-012473 are responsive to Requests for Production 5. The documents that appear at FTC-010957 to FTC-012358, FTC-012474 to FTC-013766, and FTC-013854 to FTC-013898 are responsive to Request for Production 10. The documents that appear at FTC-011034 to FTC-011276, FTC-011305 to FTC-012112, FTC-012474 to FTC-012477, FTC-012491, FTC-012552 to FTC-012553, and FTC-013626 to FTC-013628 are responsive to Interrogatory 18.

Complaint Counsel also supplements its initial disclosures with the document located at FTC-013767 to FTC-013802.

Complaint Counsel has not collected or reviewed, other than in response to Respondent's discovery requests, any additional documents required to be produced by the Order Denying Respondent's Motion for a Rule 3.36 Subpoena (February 21, 2014). Nonetheless, documents that are relevant to the Complaint's allegation that "since 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks" appear in this production at FTC-011305 to FTC-011312, FTC-011841 to FTC-011874, FTC-012347 to FTC-012358, FTC-012478 to FTC-012490, FTC-012520 to FTC-012544, FTC-013626 to FTC-013628, FTC-013762 to FTC-013766, and FTC-013897 to FTC-013898.

Please note that certain documents have been marked "Confidential," pursuant to Paragraph 6 of the Protective Order. In particular, FTC-012363 is a native audio file and as such the contents could not be stamped "Confidential." The placeholder .TIF and the metadata, as well as the accompanying static document at FTC-012362, have been marked "Confidential" to indicate that the entire document is to be treated as confidential as described in Paragraphs 7 to 13 of the Protective Order. The document at FTC-013767 to FTC-013802 has also been marked confidential.

Please notify me when you have received the enclosed disc and I will then send you the encryption key.

Sincerely,

Laura Riposo VanDruff

Enclosure

cc: Reed D. Rubinstein (*via* email)
Michael D. Pepson (*via* email)
Lorinda B. Harris (*via* email)
Hallee K. Morgan (*via* email)
Kent Huntington (*via* email)
Sunni Harris (*via* email)
Robyn Burrows (*via* email)
Daniel Epstein (*via* email)

EXHIBIT 8

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	**FILE NO. 0423160**
	)	
BJ'S WHOLESALE CLUB, INC.,	)	**AGREEMENT CONTAINING**
a corporation.	)	**CONSENT ORDER**

The Federal Trade Commission has conducted an investigation of certain acts and practices of BJ's Wholesale Club, Inc., a Delaware corporation ("proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between BJ's Wholesale Club, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent BJ's Wholesale Club, Inc. is a Delaware corporation with its principal office or place of business at One Mercer Road, Natick, Massachusetts 01760.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:

A. any further procedural steps;

B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter

may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic stripe of a credit or debit card; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with

other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, "respondent" shall mean BJ's Wholesale Club, Inc. and its successors and assigns, officers, agents, representatives, and employees.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explains how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and

D. certifies that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this seventeenth day of May, 2005

BJ's WHOLESALE CLUB, INC.

By: ____________________
BJ's WHOLESALE CLUB, INC.

____
DAVID MEDINE
JAMES W. PRENDERGAST
Wilmer Cutler Pickering Hale and Dorr LLP
Counsel for respondent BJ's Wholesale Club, Inc.

FEDERAL TRADE COMMISSION

By: ____________________
ALAIN SHEER
Counsel for the Federal Trade Commission

APPROVED:

____
JOEL WINSTON
Associate Director
Division of Financial Practices

____
LYDIA B. PARNES
Director
Bureau of Consumer Protection

Alerta de la FTC para Consumidores

Uso Compartido de Archivos:
Cómo Evaluar los Riesgos

File-Sharing: Evaluate the Risks

Todos los días millones usuarios de computadoras comparten sus archivos en línea. Ya se trate de música, juegos o programas, el uso compartido de los archivos puede permitir que todas las personas compartan una gran cantidad de información. Usted simplemente descarga un programa software especial que conecta su computadora a una red informal de otras computadoras que operan con el mismo programa. Millones de usuarios pueden conectarse a la vez entre sí por medio de este programa, el cual frecuentemente es gratuito y fácilmente accesible.

¿No es verdad que parece alentador? Quizás, pero asegúrese de considerar cuáles serán los costos que tendrá que "pagar" a cambio. La Comisión Federal de Comercio (Federal Trade Commission, FTC), la agencia nacional de protección del consumidor, advierte que el uso compartido de archivos puede acarrear una cantidad de riesgos. Por ejemplo, cuando usted está conectado a programas de uso compartido, sin darse cuenta puede estar permitiéndoles a los demás que copien archivos privados que no tiene intención de compartir. Usted puede descargar material a su computadora que está protegido por las leyes de derechos de autoría y complicarse en problemas legales. Usted puede descargar un virus informático o facilitar que se violen las medidas de seguridad en línea; o tal vez descargar involuntariamente pornografía que está presentada bajo otros títulos.

Para proteger la información personal que tiene almacenada en su computadora, la FTC le recomienda que:

- Instale el programa de uso compartido de archivos con mucho cuidado. Si al instalar el programa usted no marca las configuraciones correctas, podría estar otorgando acceso no solamente a los archivos que desea compartir sino también a otra información grabada en el disco duro de su computadora, como por ejemplo sus declaraciones de impuestos, mensajes electrónicos, registros médicos, fotos y otros documentos personales.

- Tenga cuidado con los programas de espioaje (spyware). Algunos programas de uso compartido de archivos también instalan otros programas conocidos como spyware. Este programa de espionaje monitorea los hábitos de navegación del usuario y luego envia esos datos a terceros. Algunas veces, el usuario recibe anuncios basados en la información que el spyware ha recogido y diseminado. El spyware puede ser difícil de detectar y de eliminar de su computadora. Antes de usar un programa de uso compartido de archivos es probable que desee comprar un prorgama que pueda prevenir la descarga de este tipo de spyware o que lo ayude a detectarlo en el disco duro de su computadora.

- Apague su conexión. En algunas instancias el cierre de la ventana del programa de uso compartido de archivos no cierra realmente su conexión con la red. Esto permite que continúe activado el uso compartido de archivos y podría incrementar su riesgo de seguridad. Si usted tiene una conexión de Internet de alta velocidad o "banda ancha" (high-speed o broadband connection) usted sigue conectado al Internet a menos que apague su computadora o desconecte su servicio de Internet. Este tipo de conexión permanente puede permitir que otros copien sus archivos en cualquier momento. Aún más, algunos programas de uso compartido de archivos se abren automáticamente cada vez que usted prende su computadora. Como medida preventiva, es posible que desee ajustar los controles de configuración del programa de uso compartido de archivos para evitar que se abra automáticamente.

- Utilice un programa software antivirus que sea efectivo y actualícelo regularmente. Los archivos que descarga pueden estar etiquetados incorrectamente y pueden ocultar un virus u otros contenidos indeseados. Utilice un programa antivirus para proteger su computadora contra los virus que pudieran provenir de los otros usuarios a través del programa de uso compartido. No todos los antivirus bloquean los archivos descargados a través de programas de uso compartido, así que debe verificar las capacidades de su programa antivirus y los ajustes (settings) que tiene. Además, debe evitar descargar archivos con extensiones del tipo .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, y .cmd.

- Hable con su familia sobre el tema del uso compartido de los archivos. Es posible que los padres no estén al tanto de que sus hijos descargaron programas que operan en red compartiendo los archivos de la computadora familiar y que tal vez puedan haber intercambiado, juegos, videos, música, pornografía u otro material que podría ser inapropiado para ellos. También puede suceder que, como algunas veces los archivos de otras personas pueden estar etiquetados incorrectamente, los niños los descarguen involuntariamente. Además, quizás los niños no estén en condiciones de comprender los riesgos de seguridad y de otro tipo que acarrea el uso compartido de archivos y pueden instalar el programa incorrectamente permitiéndole a cualquier navegante del Internet el acceso a los archivos privados de la computadora familiar.

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información de utilidad al consumidor con el objetivo de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite ftc.gov/espanol o llame sin cargo al
1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor (Consumer Sentinel) que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero

Julio 2005

EXHIBIT 9

United States of America
Federal Trade Commission

The Procrustean Problem with Prescriptive Regulation

Remarks of Maureen K. Ohlhausen[1]
Commissioner, U.S. Federal Trade Commission

Sixth Annual Telecom Policy Conference
Free State Foundation
Washington, DC

March 18, 2014

I. Introduction

Thank you to the Free State Foundation for inviting me to speak today. I am honored to participate in today's thoughtful discussion on the future of communications regulation.

At the Federal Trade Commission ("FTC"), protecting consumers and competition on the Internet is a substantial and growing part of our work, and I have some specific ideas on the FTC's future role. After introducing the work of the FTC, I will make three points today. First, to protect consumers effectively while promoting innovation, regulators must embrace regulatory humility and focus on consumer harm. Next, the recent *Verizon* decision is an example of the difficulties of using prescriptive *ex ante* rulemaking to regulate a dynamic industry.[2] The Greek myth of Procrustes and his iron bed is instructive here, as I will explain. Finally, reformers

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

[2] *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. Jan. 14, 2014).

"unfair and deceptive acts."[23] The Act applies across all industries with a few exceptions. And where the FCC's regulations generally set the boundaries of what certain types of entities can do, the FTC's statute fences off deceptive or unfair practices for all entities, but generally permits everything else. The FTC's process is enforcement-centric rather than rulemaking-centric. As such, it is *ex post* rather than *ex ante* and case-by-case rather than one-size-fits-all. And because an enforcement action requires a complaint and a case to move ahead, the FTC's method typically focuses on actual, or at least specifically alleged, harms rather than having to predict future harms more generally.

Because of these structural differences, the FTC's enforcement process is less affected by the systemic knowledge problems of the FCC's prescriptive *ex ante* rulemaking approach. First, rather than having to collect detailed knowledge about an entire industry, the FTC need only gather enough information about the specific parties to the dispute and their behaviors in the relevant market. The FTC has significant investigatory authority to gather such information. Second, collecting such information is much simpler because the vast majority of the necessary information will be in the hands of the parties to the case. Third, even in rapidly changing industries, the FTC's decision on a case will bind only those parties to the specific case. The case will have precedential value, but when the FTC weighs that precedent in future cases, it can then consider any changes in the underlying facts.

Thus, the FTC's approach facilitates what Adam Thierer calls "permissionless innovation," or the "anti-precautionary principle" better than a prescriptive rulemaking approach.[24] The proof, as they say, is in the pudding. As the Internet has become an

[23] 15 U.S.C. § 45(a)(1).

[24] *See* Adam Thierer, *Who Really Believes in "Permissionless Innovation"?*, http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation/ (last visited Mar. 18, 2014).

increasingly integral part of society, the FTC's enforcement-centric approach has enabled it to serve an increasingly large role in protecting consumers and competition online even while the industry has continued to innovate. In fact, the FTC is already addressing major Internet-centric concerns, including new issues in privacy, fraud, advertising and other consumer protection issues, along with competition issues.

Perhaps the most significant Internet issue the FTC has tackled is privacy. The FTC leads the federal effort to protect the privacy of consumers online. Online privacy is a very wide-ranging topic, covering spam email, data collection and security, safety of children, and online advertising. Hot new topics include the Internet of Things and big data. The FTC has been active in all of these areas, using a full range of tools, including enforcement, consumer and business education, policy research, and convening stakeholders for discussion.

For example, the FTC has brought a wide range of enforcement cases addressing consumer harms related to the Internet, including more than 100 spam and spyware cases and 50 data security cases. The FTC has brought these cases against a wide range of defendants, including an international hotel chain, a major data broker, a national drugstore chain, and the social media site, Twitter. We also hold companies to the promises made in their privacy policies and have brought actions against companies such as Google and Facebook for violating those promises. Additionally, we have brought over 20 cases to enforce the Children's Online Privacy Protection Act and have collected more than $7 million in civil penalties.[25] I believe this strong enforcement record reflects the FTC's readiness and capability to protect consumer privacy online in the face of technological change.

[25] *See generally,* Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, *Forum for EU-U.S. Legal- Economic Affairs*, Remarks at The FTC's Privacy Agenda for the 2014 Horizon (September 14, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/ftc%E2%80%99s-privacy-agenda-2014-horizon-forum-eu-u.s.legal-economic-affairs/130914berlinprivacyin2014.pdf.

Enforcement is the cornerstone of our activity to protect consumers online. But it is supported by a wide range of other complementary tools that the FTC uses to promote consumer welfare and competition online, including consumer and business education and policy R&D efforts.

In some respects, the Commission's consumer and business education efforts affect a greater percentage of American consumers than anything else we do. For example, the information available on our webpages to help consumers avoid becoming victims of identity theft and to mitigate the damage of identity theft have had millions of hits and has been distributed widely in hardcopy. We also educate consumers on how to avoid falling victim to online scams, how to deal with spam email, how to protect their computers, phones, and home networks, and how to keep children safe online, among many other topics. For businesses we offer a wide range of legal resources, guidance, and handbooks on topics including online advertising, privacy laws, and best practices across the Internet, including websites, mobile apps, and general data security.

The FTC also has a strong policy research and development capability that it uses to stay abreast of new technologies and emerging issues. For example, the Commission has been closely studying the related issues of big data and the Internet of Things. The FTC has hosted successful workshops on these topics and others, including disclosures of online marketing and advertising practices, children's online privacy and new technology, and mobile device tracking. Future FTC workshops will cover topics such as consumer behavioral prediction and analysis and consumer generated health data. These workshops are particularly valuable because not only do they educate consumers and businesses, they also help the Commission stay informed about the ongoing technological developments and the benefits and risks of such new technologies.

EXHIBIT 10

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

In the Matter of:)
LabMD, INC., a corporation) Docket No.
Respondent.) 9357

- - - - -

DEPOSITION OF DANIEL KAUFMAN
Washington, D.C.
Monday, April 14, 2014

The deposition of DANIEL KAUFMAN was convened on Monday, April 14, 2014, commencing at 10:42 a.m., at the offices of the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C., before Karen K. Brynteson, Registered Merit Reporter, Certified Realtime Reporter, and Notary Public.

- - - - -

Page 115

to allegations of consumer injury. So you can answer to the extent you know.

THE WITNESS: Yeah, I do think that the allegations all focus on natural persons, so yes.

MR. SHERMAN: Okay. I need to take a break.

(A recess was taken at 2:32 p.m., after which the deposition resumed at 2:40 p.m.)

MR. SHERMAN: Back on the record. I want to place this on the record, counsel.

My next line of inquiry would be to question Mr. Kaufman and the Bureau about the data security standards that they are going to use to basically demonstrate that LabMD participated in an unfair practice.

It is my understanding that you have made an objection to that line of inquiry.

MS. VAN DRUFF: I believe that the Court had made a determination that that line of inquiry is not permissible.

MR. SHERMAN: Okay. I think I just

Page 116

want to place on the record that I disagree with your objection. I believe that what the Court stated was that we could not require -- inquire generally into legal standards, and this is on page 7, second -- the first full paragraph, that we could not -- that we could not inquire generally into the legal standards of the FTC used in the past, and it is currently using to determine whether an entity's data security practices are unfair under Section 5.

I do not believe that it prevents us from inquiring about the data security standards. And that is where I want to go next with Mr. Kaufman. And I understand you may have an objection, but I submit that for your consideration.

MS. VAN DRUFF: And you are drawing a distinction between the language on page 7 of the Court's March 10th order and the language on page 9 at numbered paragraph 3 of the Court's order; is that correct?

MR. SHERMAN: Yes. I am not asking

Page 117

about their decision-making. I want to know what standard LabMD is going to be held to throughout the period.

The data security standard, not the legal standard, not reasonableness.

MS. VAN DRUFF: Okay. And so to be clear, counsel, if you were to frame your question in terms of the factual bases of the allegations of paragraph 10, which has several subparagraphs, I may be able to permit Mr. Kaufman to answer, but otherwise -- and that is consistent with the Court's holding on page 6 of the March 10th opinion.

MR. SHERMAN: The other question, counsel, is given your narrow interpretation of the Judge's order, I know that you have probably prepared your witness based on your interpretation of that order. Is Mr. Kaufman prepared to respond to questions which would ask him what the data security standards are for certain time periods that LabMD will be measured up against?

Page 118

MS. VAN DRUFF: I can't begin to answer that question in the abstract. I would need to know what the question was, and then that may go to a privilege, so I don't know that I can submit to you whether Mr. Kaufman was prepared on a specific subject or not by counsel.

MR. SHERMAN: Okay.

BY MR. SHERMAN:

Q. Mr. Kaufman, paragraph 10 of the Bureau's complaint indicates that at all relevant times LabMD engaged in a number of practices that taken together failed to provide reasonable and appropriate security for personal information on its computer networks.

Among other things in paragraph A it says that, it alleges that LabMD did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information.

And I am reading from the complaint. Do you have a copy of the complaint?

Page 119

A. No.

Q. We didn't provide you with a copy of the complaint? I had a copy of the complaint for everyone.

(Deposition Exhibit Number RX-9 was marked for identification.)

MS. VAN DRUFF: I'm sorry, counsel, was there a question pending?

MR. SHERMAN: No. I wanted to make sure that the witness had a copy of the complaint in front of him.

BY MR. SHERMAN:

Q. Based on the allegations in paragraph 10(a), my question is has the Bureau or the FTC published, and by published I mean made available to the public, the standard that it requires for a comprehensive information security program for companies like LabMD to have in place?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I

Page 120

am instructing Mr. Kaufman to not answer the question.

If you would like to reframe the question as it relates to paragraph 10(a), in terms of the factual bases of Complaint counsel's allegations, I will permit Mr. Kaufman to answer.

MR. SHERMAN: Okay.

BY MR. SHERMAN:

Q. So is there a factual bases for the allegation that LabMD did not develop, implement, or maintain a comprehensive information security program that met the data security standards set out by the Bureau during the year of 2005?

MS. VAN DRUFF: And I would make the same objection and the same instruction. Again, at note 6 of the Court's order, the Judge acknowledges that it has already -- that, I'm sorry, the Court has rejected LabMD's argument that it is entitled to discovery of the standards the Commission used in the past and is

Page 121

currently using to determine whether an entity's data security practices violate Section 5.

So if you would like to inquire of Mr. Kaufman the factual bases of the allegation of paragraph 10(a), you may ask that question, but as it relates to standards, I will instruct Mr. Kaufman --

MR. SHERMAN: I want to know -- I am not going to change my question.

BY MR. SHERMAN:

Q. I want to know what the data security standards are, okay, and were for the year 2005, that the Bureau published and made known to companies like LabMD with regard to implementing, developing, maintaining a comprehensive information security program to protect consumers' personal information?

MS. VAN DRUFF: And I am lodging the same objection. That question exceeds the bounds of the Court's protective order. And I am instructing Mr. Kaufman to not answer the question.

Page 122

BY MR. SHERMAN:

Q. And I would ask the same question for the year 2005, 2006, 2007, 2008, 2009, 2010, and through the years to the present for each subcategory in paragraph 10.

So, in other words, my question is were the data security standards published and made known to companies like LabMD that the Bureau and/or the FTC made known that establish what a company should do and to what extent it should develop, implement, and maintain a comprehensive information security program to protect consumers' personal information? I would go to subparagraph 10(b), what did the Bureau do and what were the standards that the Bureau published and made known to companies like LabMD requiring them to use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks from the year 2005 through the present, and I would ask a similar question for each subcategory in

Page 123

paragraph 10.

And so is it still your position that you would object to each of those questions and instruct Mr. Kaufman not to answer?

MS. VAN DRUFF: Without a pending question, I don't know that I can respond to that, but what I can tell you is the question as it is formulated as I understand it relating to A and B exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer that question.

MR. SHERMAN: I will go through each question then, okay?

MS. VAN DRUFF: Okay.

BY MR. SHERMAN:

Q. So just to be clear, Mr. Kaufman, I would like to know what are the data security standards that were published in any way, shape, form, or fashion by the Bureau or the FTC that were available and were made known to companies like LabMD about what the FTC's standards or requirements were for the use of readily available measures or what those readily available measures to identify commonly known and reasonably foreseeable security risks and vulnerabilities on its networks were? Can you answer that question?

And please keep in mind I am asking for an answer that would encompass the time period of 2005 through the present.

MS. VAN DRUFF: And I object to the question on the basis that it is vague, ambiguous, and compound, and that it most importantly exceeds the bounds of the Court's March 10th, 2014 protective order, which limited the topics of this deposition. And I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, can you tell us what data security standards were published by the Bureau or the FTC to make known to companies like LabMD what the Bureau or the FTC expected in terms of

Page 125

data security standards for that company as it relates to the adequate measures to prevent employees from accessing personal information not needed to perform their jobs?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order insofar as it does not relate to any of the four topics noticed by Respondent and limited by the Court's order, and I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. And, again, I would couch that question for the period of 2005 through the present, and I would note your objection.

MS. VAN DRUFF: The same objection, same instruction to not answer the question because it exceeds the bounds of the protective order.

BY MR. SHERMAN:

Q. Mr. Kaufman, can you tell us what the data security standards are that the FTC

Page 126

published or made known to companies like LabMD which would establish a standard for companies like LabMD to adequately train employees to safeguard personal information from 2005 through the present?

MS. VAN DRUFF: Object to the question on the basis that it exceeds the bounds of the Court's March 10th, 2014 protective order. And I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, what is the standard that the FTC has established, published, and put forth which informs companies like LabMD what the FTC expects with regard to that company's requiring employees or other users with remote access to the networks to use commonly authenticated -- I'm sorry, common authentication-related security measures such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication?

Page 127

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10, 2014 protective order. And I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. From the period of 2005 through 2010. I'm sorry, from 2005 to the present. And I note your objection.

MS. VAN DRUFF: Same objection, continued instruction. Thank you, counsel.

BY MR. SHERMAN:

Q. Mr. Kaufman, what are the standards, the data security standards established by the Bureau or the FTC which the Bureau has made known or published and made known to companies like LabMD advising them that the FTC's expectation -- advising them as to what the FTC's expectations were with regard to maintaining and updating operating systems of computers and other devices on its networks, for example, on some computers, Respondent used

Page 128

operating systems that were unsupported by the vendor.

Were there any such data security standards and regulations published and made known by the Bureau or the FTC which would advise a company like LabMD what those standards were?

MS. VAN DRUFF: Object to the question, which is compound and ambiguous, but also because it exceeds the bounds of the Court's March 10th, 2014 protective order. And I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. And I would include from 2010 through the present.

MS. VAN DRUFF: It is the same instruction, same objection.

BY MR. SHERMAN:

Q. Mr. Kaufman, what are the data security standards established or published, and/or published by the FTC which would inform a company such as LabMD what the FTC's expectations were with regard to that company employing readily available measures to prevent or detect unauthorized access to personal information on its computer networks from 2005 through the present?

MS. VAN DRUFF: Object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order. And I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, has the FTC or the Bureau informed entities like LabMD that the FTC expects or requires them to have a comprehensive information security program?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's protective order. And I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, has the Bureau or the FTC

Page 130

informed entities like LabMD that the FTC expects and/or requires them to use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman not to answer.

BY MR. SHERMAN:

Q. Mr. Kaufman, has the FTC informed entities like LabMD that the FTC expects or requires them to use adequate measures to prevent employees from assessing personal information not needed to perform their jobs?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, has the Bureau or the FTC

Page 131

informed entities like LabMD that the FTC expects or requires them to use appropriate measures to prevent employees from installing on their computers applications or materials that were not needed to perform their jobs?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, has the Bureau or the FTC informed entities like LabMD that the FTC expects or requires them to use appropriate measures to adequately maintain or review records of activities on their networks?

MS. VAN DRUFF: Object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Page 132

Q. Mr. Kaufman, where can a company like LabMD find the Bureau's or the FTC's data security standards which will inform a company like LabMD what the FTC or the Bureau expects with regard to that company's data security?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, with regard to data security standards, does the Bureau or the FTC have the authority to enforce HIPAA?

MS. VAN DRUFF: Objection, counsel. Are you grounding any -- are you grounding your question in any of the topics noticed by Respondent or as limited by the Court's March 10th, order?

MR. SHERMAN: Yes. And it is the objectionable topic of data security standards.

MS. VAN DRUFF: I see.

Page 133

MR. SHERMAN: The topic which you have been objecting to.

MS. VAN DRUFF: Thank you, counsel. May I have the question read back, please?

THE REPORTER: "Question: Mr. Kaufman, where can a company like LabMD find the Bureau's or the FTC's data security standards which will inform a company like LabMD what the FTC or the Bureau expects with regard to that company's data security?"

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question.

BY MR. SHERMAN:

Q. With regard to data security, does the Bureau or the FTC have the authority to enforce HITECH?

MS. VAN DRUFF: I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I

Page 134

am instructing Mr. Kaufman to not answer the question.

MR. SHERMAN: Can we go off the record?

MS. VAN DRUFF: Certainly.

MR. SHERMAN: I need to take a break and consult with my counsel.

MS. VAN DRUFF: Of course.

(A recess was taken at 3:05 p.m., after which the deposition resumed at 3:06 p.m.)

BY MR. SHERMAN:

Q. Mr. Kaufman, I am going to show you what has been marked as RX-10, which for the record is the expert report of Raquel Hill.

(Deposition Exhibit Number RX-10 was marked for identification.)

BY MR. SHERMAN:

Q. Have you seen that document before?

A. Yes.

Q. Are the requirements set out in Professor Hill's report what the Bureau will measure LabMD's performance in terms of its data

Page 135

security against at the hearing?

MS. VAN DRUFF: I'm sorry, I am going to need the question read back.

THE REPORTER: "Question: Are the requirements set out in Professor Hill's report what the Bureau will measure LabMD's performance in terms of its data security against at the hearing?"

MS. VAN DRUFF: And, counsel, not trying to be difficult but, of course, the Bureau is not the fact finder at the hearing, so is your question what the Bureau's standard will be at the hearing?

BY MR. SHERMAN:

Q. Well, my question is you would agree that in Professor Hill's report, there are several descriptions of what Professor Hill opines to be adequate data security measures that should have been taken by LabMD in order to adequately protect the information that it possessed, correct?

MS. VAN DRUFF: Objection, Professor

Page 136

Hill's report speaks for itself, but you may answer the question.

THE WITNESS: That's my understanding, yes.

BY MR. SHERMAN:

Q. Okay. And you have read the -- you have reviewed the report, correct?

A. Correct.

Q. Okay. My question is is that the data security standard that LabMD will be held to in terms of whether or not its data security practices and procedures from 2005 through, I think, July of 2010, is that what -- is that the standard that LabMD will be held to at the hearing?

MS. VAN DRUFF: And, counsel, questions relating to standards exceed the bounds of the Court's March 10th, 2014 protective order. To the extent you want to rephrase your question as it relates to factual bases for the allegations of paragraph 10, I will permit Mr. Kaufman to answer, but otherwise

Page 137

I am instructing Mr. Kaufman to not answer the pending question.

BY MR. SHERMAN:

Q. Mr. Kaufman, if it is demonstrated at the hearing that -- well, let me ask you this: The requirement set out in Professor Hill's report with regard to data security, does the Bureau intend to apply these particular standards to other companies?

MS. VAN DRUFF: And, again, counsel, to the extent that your question relates to standards or the investigational prosecution of other targets, it exceeds the bounds of the Court's March 10th, 2014 protective order. And I am instructing Mr. Kaufman not to answer the question.

BY MR. SHERMAN:

Q. Mr. Kaufman, in terms of the data security standards set out in Professor Hill's report, is it the Bureau's position that if LabMD did not take every measure set out in this report, that LabMD has committed an unfair act

Page 138

or practice?

MS. VAN DRUFF: Can I have the question read back, please?

THE REPORTER: "Question: Mr. Kaufman, in terms of the data security standards set out in Professor Hill's report, is it the Bureau's position that if LabMD did not take every measure set out in this report, that LabMD has committed an unfair act or practice?"

MS. VAN DRUFF: The question is predicated on data security standards, and as such it exceeds the bounds of the Court's March 10, 2014 protective order, and I am instructing Mr. Kaufman to not answer that question.

MR. SHERMAN: Based on that, counsel, I don't have any further questions. What I would like to do is to attempt, at least, to get the ALJ on the phone, not today but some day where we can discuss whether or not your objections will be sustained to that line of questioning.

And so that's, that's my intent.

Page 139

MS. VAN DRUFF: Thank you, counsel.

MR. SHERMAN: Thank you, Mr. Kaufman.

THE WITNESS: Thank you.

(Whereupon, at 3:12 p.m., the deposition was concluded.)

EXHIBIT 11

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

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

COMPLAINT COUNSEL'S ANSWER AND OBJECTIONS TO RESPONDENT'S FIRST SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS (NUMBERS 1-17)

Pursuant to Sections 3.31 and 3.37 of the Federal Trade Commission's Rules of Practice, Complaint Counsel hereby responds to Respondent LabMD, Inc.'s First Set of Requests for the Production of Documents ("Respondent's Requests"). Subject to the General and Specific Objections below, and without waiving these objections, Complaint Counsel answers as follows:

General Objections

The following General Objections apply to each request for documents in Respondent's Requests and are hereby incorporated by reference into each response. The assertion of the same, similar, or additional objections or the provision of partial answers in response to an individual request does not waive any of Complaint Counsel's General Objections as to the other requests.

1. Complaint Counsel objects to Respondent's Requests to the extent they seek to impose duties and obligations upon Complaint Counsel beyond those imposed by the Commission's Rules of Practice for Adjudicative Proceedings, including seeking documents that are beyond the scope of permissible discovery under Rule 3.31(c)(2).

8. All documents sufficient to show what data-security standards are currently used by FTC to enforce the law under Section 5 of the Federal Trade Commission Act.

Complaint Counsel refers Respondent to its response to Document Request 10.

9. All documents sufficient to show what changes occurred in the data-security standards used by FTC to enforce the law under Section 5 of the Federal Trade Commission Act from 2005 to the present and the dates on which these standards changed.

Complaint Counsel objects to this Document Request as vague and ambiguous.

Complaint Counsel refers Respondent to its response to Document Request 10.

10. All documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present.

In addition to the General Objections, Complaint Counsel specifically objects to this Document Request to the extent it seeks to impose duties and obligations upon Complaint Counsel beyond the Commission's Rules of Practice for Adjudicative Proceedings. Complaint Counsel further objects that any such documents unrelated to the FTC's investigation of LabMD and preparations for this hearing are not relevant to the allegations of the Complaint, to the proposed relief, or to the defenses asserted by Respondent. Complaint Counsel further objects to this Document Request as overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence, and an improper inquiry into the mental processes of the Commissioners and FTC attorneys.

To the extent this Document Request seeks information in the possession, custody, or control of the Commissioners, the General Counsel, or any Bureau or Office not involved in this matter, Complaint Counsel further objects to this Document Request. Documents in the possession, custody, or control of the aforementioned entities must be sought through written motion under the procedure laid out in Rule 3.36, 16 C.F.R. § 3.36.

Complaint Counsel further objects to this Document Request to the extent it seeks documents that are protected by the work product doctrine, government deliberative process privilege, government informer privilege, law enforcement investigatory privilege, or common interest privilege.

Complaint Counsel further objects to this Document Request as vague and ambiguous.

Subject to and without waiving any General or Specific objections, Complaint Counsel states that is has previously produced responsive, discoverable, and non-privileged documents at FTC-000685 to FTC-000893and will produce responsive, discoverable, and non-privileged documents.

11. All documents provided to the FTC pursuant to any Civil Investigation Demand regarding its investigation of LabMD.

In addition to the General Objections, Complaint Counsel specifically objects to this Document Request to the extent it seeks to impose duties and obligations upon Complaint Counsel beyond the Commission's Rules of Practice for Adjudicative Proceedings. Complaint Counsel further objects that any such documents unrelated to the FTC's investigation of LabMD and preparations for this hearing are not relevant to the allegations of the Complaint, to the proposed relief, or to the defenses asserted by Respondent. Complaint Counsel further objects to this Document Request as overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence, and an improper inquiry into the mental processes of the Commissioners and FTC attorneys.

Complaint Counsel further objects to this Document Request to the extent it seeks documents that are protected by the work product doctrine, government deliberative process privilege, government informer privilege, law enforcement investigatory privilege, or common interest privilege.

Complaint Counsel further objects to this Document Request to the extent the requested documents that were provided by Respondent can be obtained directly by Respondent through less burdensome means.

Complaint Counsel further objects to this Document Request to the extent it seeks production of materials previously produced to Respondent.

Subject to and without waiving any General or Specific objections, Complaint Counsel states that it has previously produced responsive, discoverable, and non-privileged documents at FTC-PRI-000001 to FTC-PRI-001724 and refers Respondent to the documents Respondent produced, which have been Bates labeled FTC-LABMD-000001 to FTC-LABMD-003851.

12. All documents identifying LabMD and other companies whose documents or files Tiversa downloaded from Peer to Peer Networks which contained Personal Identifying Information and or Protected Health Information that were provided to FTC.

In addition to the General Objections, Complaint Counsel specifically objects to this Document Request to the extent it seeks to impose duties and obligations upon Complaint Counsel beyond the Commission's Rules of Practice for Adjudicative Proceedings. Complaint Counsel further objects that any such documents unrelated to the FTC's investigation of LabMD and preparations for this hearing are not relevant to the allegations of the Complaint, to the proposed relief, or to the defenses asserted by Respondent. Complaint Counsel further objects to this Document Request as overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence, and an improper inquiry into the mental processes of the Commissioners and FTC attorneys.

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LabMD, INC.,	)	
	)	
Plaintiff,	)	
v.	)	
	)	Civil Action No.: 1:14-CV-810-WSD
FEDERAL TRADE COMMISSION,	)	
	)	
Defendant.	)	

EXPERT OPINION DECLARATION OF CLIFF BAKER

In accordance with 28 U.S.C. § 1746, the declarant, Cliff Baker states:

1. I am Cliff Baker. I submit this declaration for use in the lawsuit *LabMD v. Federal Trade Commission.* I offer this declaration to respond to statements in the Expert Report of Professor Hill and how her opinions on data security relate to requirements on data security for HIPAA-covered medical service providers imposed by the Department of Health and Human Services. HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. I base my declaration on my personal knowledge and professional experiences.

2. I, Cliff Baker, have had the following roles in my career in the field of data security:

a. Director in the Healthcare Information Security practice at PricewaterhouseCoopers. I led the security practice nationally for the Healthcare Consulting practice. I worked at PricewatershouseCoopers for 14 years and consulted with clients nationally on implementing security programs and practices. An example of a project I led was a establishing a program that included four state healthcare associations. The program included meeting, discussing and educating over 50 organizations on adopting security measures to comply with HIPAA.

b. Chief Strategy Officer for HITRUST. I joined HITRUST in 2008 to lead the creation of the Common Security Framework, which is a healthcare industry framework based on globally recognized standards, such as ISO 27001/2 and NIST. A key objective of the framework is to provide a prescriptive and scalable reference for covered entities to determine reasonable and appropriate controls to implement for their organizations. The controls are tailored to the size and operations of the organization. I facilitated working sessions with over 200 security professionals from the healthcare industry, security technology companies, consulting companies, and government entities in the development of the framework.

c. Founder and Managing Partner of Meditology Services. Meditology Services was founded in 2010 to provide privacy and security services to healthcare clients. I employ former Chief Information Security and Privacy Officers that were responsible for implementing security at their healthcare organizations. We provide consulting services in the areas of compliance with HIPAA and the implementation of privacy and security programs for healthcare organizations ranging from small providers to global healthcare organizations.

3. I have spent over 19 years working in the healthcare and information security fields. This experience has provided me with first-hand knowledge about the challenges and practical realities faced by healthcare organizations in securing Protected Health Information (PHI).

4. The 1996 HIPAA Statute states that in promulgating information security regulations, the Secretary must take into account "the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary)," and the preamble to the HIPAA Security

Rule (p. 8335) states accordingly that one of the foundations of the rule is that "it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes."

5. The process by which HHS promulgated the initial final HIPAA Security Rule involved reviewing and responding to approximately 2,350 timely public comments, balancing the interests of health care professionals and firms with patient-related interests. Based on these public comments, HHS crafted a unique information security regulatory scheme that separated "implementation specifications" – the types of very specific security requirements emphasized by the FTC's expert – into two classes: "required" and "addressable". HHS stayed consistent with this structure in its most recent updates to the HIPAA Privacy and Security rules in 2013. This structure reflects HHS' challenge in complying with Congressional intent in establishing a security rule to address reasonable and appropriate security requirements for the range of organizations in healthcare that differ greatly in operations, size, complexity, and resources. For example, a single physician practice may differ significantly from the way in which it addresses security as compared to a multi-national health plan. The physician practice will probably not employ dedicated technology or security personnel and will rely heavily on guidance from HHS. The practice will also rely predominantly on

security that is provided by default settings and software vendor recommendations and will implement mostly manual procedures to manage and monitor access to patient information and associated Information Technology (IT) systems. On the other end of the spectrum, a national health system will likely hire a team of experienced security professionals that may even exceed the total number of employees in these small practices. These larger organizations will buy and build the most advanced and sophisticated solutions available in their efforts to protect sensitive patient data.

6. HIPAA demands that a covered entity perform a risk assessment in good faith and take actions to secure Electronic Protected Health Information (EPHI) based on the findings of that risk assessment. HIPAA's security requirements are also explicitly "scalable" based on the size of the entity. Therefore, to assess HIPAA noncompliance, it is necessary to determine if a risk assessment was performed in good faith, and resulted in a process that included implementation of requirements and appropriate responses to "addressable" issues. These responses are all subject to different standards and scalable so that they could be implemented effectively by covered entities of all types and sizes. Given the limited knowledge of information technology by many small health care providers, especially during the early years of HIPAA Security,

many of the security measures they were advised to adopt by HHS issued guidance related to physical and administrative security rather than specific technical security.

7. The preamble to the Rule makes the balancing of interests and the assessment of feasibility for small providers by HHS, employing notice and comment rulemaking, quite transparent at many points. For example, in connection with encryption of data in transit, which corresponds to Section 164.312(e)(1) of the Rule on Transmission Security, the preamble notes (FR V. 68, #34 at 8357):

> [W]e agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting email communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification.

8. This concept was reinforced by CMS in a seven-part series published to provide guidance to the industry for complying with HIPAA. In Volume 2 Security Standards: Implementation for Small Provider of the HIPAA Security Series published in December 2007, CMS states:

> All covered entities must comply with the applicable standards, implementation specifications, and requirements of the Security Rule with respect to EPHI (see 45 C.F.R § 164.302.). Small providers that are covered entities have unique business and technical environments that provide both opportunities and challenges related to compliance with the Security Rule. As such, this paper provides general guidance to providers such as physicians and dentists in solo or small group practices, small clinics, independent pharmacies, and others who may be less likely to have IT staff and whose approach to compliance would generally be very different from that of a large health care system. It is important to note however, that this paper does not define a small provider, nor does it prescribe specific actions that small providers must take to become compliant with the Security Rule.

9. These comments reflect the challenges of small providers in the early years of HIPAA, but even as more recently as 2013 and 2014, HHS is still publishing security guidance for small providers, and the guidance is still elementary in nature. This is reflected by the following list of recommendations published in the most recent version of the Guide to Privacy and Security of Health Information, published by the Office of the National Coordinator for Health Information Technology in 2013:

> Remember the Basics
>
> - Is your server in a room only accessible by authorized staff? Do you keep the door locked?
> - Are your passwords easily found (e.g., taped to a monitor)? Easy to guess?

- Do you have a fire extinguisher that works?
- Where, when, and how often do you back-up? Is at least one back-up kept offsite? Can your data be recovered from the back-ups?
- How often is your EHR server checked for viruses?
- Who has keys to your building? Any former employees or contractors?
- What is your plan for what to do if your server crashes and you cannot directly recover data? Do you have documentation about what kind of server it was, what software it used, etc.?

10. These recommendations reflect HHS' understanding of the realities associated with implementing security for small providers in the healthcare industry. After almost ten years of complying with HIPAA security rules, the guidance has not changed substantively for small practices. In more recent years, HHS has focused on requiring security functionality to be built into applications for the healthcare industry, so providers will have many security controls by default and not have to rely on expertise, additional tools and resource intensive processes to protect information.

11. I have reviewed Dr. Hill's Report, and believe that the standards articulated by Dr. Hill are:

a. Confusing by introducing additional security principles (i.e., 7 security principles referenced by Dr. Hill) that are difficult to reconcile with the Administrative, Technical and Physical main structure of the HIPAA security rule.

b. Not scalable in accordance with the Security Rule, and not taking account as required by the 1996 HIPAA Statute of "the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary). For example, the recommendation for file integrity monitoring requires expertise to implement and configure these solutions and can be even more resource intensive to understand, investigate and resolve alerts produced by the solution. In my experience, I very rarely observe adoption of this technology by small providers in the industry.

c. More prescriptive than HIPAA or inconsistent with HHS guidance, including encryption at rest (an addressable requirement of 164.312(a)(1)), encryption in transit (an addressable requirement of 164.312(e)(1)), intrusion detection (not addressed specifically by the Security Rule), virus protection (an addressable requirement of 164.308(a)(5) (ii)(B)), firewalls (not addressed specifically by the Security Rule), penetration testing (not addressed by the Security Rule), and file integrity monitoring (not addressed specifically by the Security Rule). While many of these standards are good security practices, controls such as broad scale encryption at rest are generally not adopted across the industry. The electronic health record certification requirements published for HHS for Meaningful Use Stage 2 in 2012 do not even require this level of encryption for all PHI stored by the system. In addition, tools such as intrusion detection and file integrity monitoring systems require experienced and committed technical resources to configure and manage. Dr. Hill's standards presume a level of knowledge of technical information security generally not available to small health care providers.

d. Contradictory to the guidance provided by HHS. For example, Dr. Hill almost exclusively focuses on technologies or technical processes for the risk assessment process (i.e., antivirus applications, firewalls, various types of vulnerability scans, intrusion detection systems, penetration tests, file integrity monitoring, and other measures). This is inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process as outlined in the standard referenced by Dr. Hill: Special Publication NIST 800-30 Guide for Conducting Risk Assessments.

12. If health care providers are going to be held to a compliance standard that is simply an expert's opinion of best practices in information security at any point in time, when that expert standard exceeds the published compliance standard developed under HIPAA and the historical guidance provided by HHS, then the standard developed under HIPAA is made effectively meaningless. This will create confusion for Health care providers that will not know what is required of them.

13. I have not reviewed whether LabMD is or was compliant with the HIPAA Security Rule; I suggest only that for HIPAA not to be contradicted and Congressional intent and constitutional process not to be undermined, the information security of HIPAA-covered health care providers must be regulated by an agency with jurisdiction under the properly promulgated HIPAA Security Rule,

which during the time period in question was only the Department of Health and Human Services.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 11 day of April, 2014.

CLIFF BAKER

CERTIFICATE OF SERVICE

This is to certify that, on April 11, 2014, I electronically filed the foregoing **EXPERT OPINION DECLARATION OF CLIFF BAKER** with the Clerk of Court using the CM/ECF system, and served the following by e-mail and U.S. Mail as follows:

LAUREN E. FASCETT, Esq.
Trial Attorney
U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Lauren.Fascett@usdoj.gov

This 11th day of April, 2014.

/s/ Burleigh L. Singleton
Counsel for Plaintiff