FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
05 07 2014
569816
SECRETARY

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

COMPLAINT COUNSEL'S SEPARATE AND CONCISE STATEMENT OF MATERIAL FACTS AS TO WHICH THERE EXIST GENUINE ISSUES FOR TRIAL

Pursuant to Rule 3.24(a)(2) of the Commission's Rules of Practice, 16 C.F.R. § 3.24(a)(2), Complaint Counsel submits the following Separate and Concise Statement of Material Facts as to which there Exist Genuine Issues for Trial ("Separate Statement"). Part I of this submission sets forth those material facts (with citations to supporting admissible evidence) as to which there is a genuine issue. Part II sets forth statements Respondent has characterized as undisputed and Complaint Counsel's responses to the statements.

PART I: STATEMENT OF MATERIAL FACTS AS TO WHICH THERE EXISTS A GENUINE ISSUE FOR TRIAL

Respondent's Security Practices

1. Respondent did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Ans. ¶ 10 (attached as Exhibit 1); Expert Report of Raquel Hill, Ph.D. ("Hill Report") ¶¶ 52, 61 (attached as Exhibit 2); Rebuttal Report of Raquel Hill, Ph.D. ("Hill Rebuttal") ¶¶ 7-10 (attached as Exhibit 3); Invest. Hrg. Tr. of J. Boyle, LabMD Designee (Feb. 5, 2013) at 78-79, 91-92 (testifying that LabMD did not have written information security policies prior to 2010) (attached as Exhibit 4).

2. Respondent did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. For example, by not using measures such as penetration tests, Respondent could not adequately assess the extent of the risks and vulnerabilities of its networks. Ans. ¶ 10 (Ex. 1); Hill Report ¶¶ 64-67, 69 (Ex. 2); Dep. Tr. of M. Daugherty, LabMD Designee (Mar. 4. 2014) at 126, 150-51 (testifying regarding records of penetration tests that first occurred in May 2010) (attached as Exhibit 5); Invest. Hrg. Tr. of C. Kaloustian (May 3, 2013) ("Kaloustian IH Tr.") at 92, 281-82 (stating that no penetration tests were performed during his time at LabMD) (attached as Exhibit 6).

3. Respondent did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs. Ans. ¶ 10 (Ex. 1); Hill Report ¶¶ 83-85 (Ex. 2); Resp't's Supplemental Resp. to Complaint Counsel's First Set of Interrogs. (Mar. 17, 2014), Resp. to Interrog. 1 and 2 (listing the LabMD employees with access to Personal Information and stating Respondent is "unable to answer" which types of Personal Information each employee had authority to access) (attached as Exhibit 7).

4. Respondent did not adequately train employees to safeguard personal information. Ans. ¶ 10 (Ex. 1); Hill Report ¶ 91 (Ex. 2); *see, e.g.*, Kaloustian IH Tr. (Ex. 6) at 62-64 (records stored in clear text; no policy on who should have access to records, and access granted *ad hoc*, resulting in most employees receiving administrative access to servers), 302-04 (information transmitted from doctor's offices unencrypted; informal policy that doctors' offices would get unique access credentials, but credentials would then be shared amongst multiple users at a practice).

5. Respondent did not require employees, or other users with remote access to Respondent's 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. Ans. ¶ 10 (Ex. 1); Hill Report ¶ 95 (Ex. 2); Kaloustian IH Tr. at 254-58 (Ex. 6) (stating that LabMD had no credential requirements, other authentication controls, or mechanism to assess the strength of users' passwords); Dep. Tr. of S. Brown (Jan. 11, 2014) at 11-15 (stating that she used the username sbrown

and password labmd across applications throughout her tenure at LabMD) (attached as Exhibit 8); Dep. Tr. of M. Bureau (Jan. 10, 2014) at 82-84 (no credential requirements) (attached as Exhibit 9); Dep. Tr. of P. Gilbreth (Feb. 7, 2014) at 67 (no password policies or procedures) (attached as Exhibit 10); Dep. Tr. of R. Hyer (Dec. 13, 2013) at 26-27 (stating that some employees shared credentials and passwords were not sufficiently complex) (attached as Exhibit 11); Dep. Tr. of B. Bradley (Feb. 14, 2014) at 7, 128-30 (stating there was no requirement to periodically change passwords when he started, in approximately May 2010) (attached as Exhibit 12).

6. Respondent did not maintain and update operating systems of computers and other devices on its networks. Ans. ¶ 10 (Ex. 1); Hill Report ¶ 100 (Ex. 2); Providyn External Vulnerability Scan, May 19, 2010 at 1, 19, 37 (identifying as an "Urgent Risk" an anonymous login vulnerability on its FTP server, for which a solution had been published in 1999, concluding that "Overall Security Posture" of the server was "Poor") (attached as Exhibit 13); Dep. Tr. of P. Howard at 34-37 (LabMD used FTP to receive Personal Information from its physician clients) (attached as Exhibit 14).

7. For example, on some computers Respondent used operating systems that were unsupported by the vendor, making it unlikely that the systems would be updated to address newly discovered vulnerabilities. Ans. ¶ 10 (Ex. 1); Hill Report ¶ 100 (Ex. 2); Kaloustian IH Tr. at 271-74 (Ex. 6) (stating that LabMD used unsupported operating systems on servers); Dep. Tr. of A. Truett (Feb. 27, 2014) at 82-84 (servers running Symantec Corporate 7, which was no longer supported) (attached as Exhibit 15).

8. Respondent 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. Ans. ¶ 10 (Ex. 1); Hill Report ¶ 105 (Ex. 2); Kaloustian IH Tr. at 90-93 (Ex. 6) (no process for risk assessment), 166-67 (administrative privileges), 173-75 (no automated scanning of desktops); Dep. Tr. of A. Simmons (Feb. 5, 2014) at 52-56 (no technical controls prevented employees from downloading file-sharing software to their computers) (attached as Exhibit 16).

9. As a result, Respondent did not detect the installation or use of an unauthorized file-sharing application on its networks. Ans. ¶ 10 (Ex. 1); Simmons Dep. Tr. at 24-25, 54-56 (Ex. 16) (LimeWire installed on billing manager's computer in 2005 or 2006; LabMD did not use tools that could have detected the installation of a P2P application); Kaloustian IH Tr. at 269-70 (Ex. 6) (LabMD did not use tools that could have prevented or detected the installation of a P2P application).

10. Respondent could have corrected its security failures at relatively low cost using readily available security measures. Ans. ¶ 11 (Ex. 1); Hill Report ¶¶ 60, 62, 68, 71, 76-77, 80, 85, 91-92, 95-96, 100-01, 104-06 (Ex. 2).

11. Consumers have no way of independently knowing about Respondent’s security failures and could not reasonably avoid possible harms from such failures, including identity theft, medical identity theft, and other harms, such as disclosure of sensitive, private medical information. Ans. ¶ 12 (Ex. 1); Expert Report of Rick Kam, Certified Information Privacy Professional (CIPP/US) (“Kam Report”) at 17 (attached as Exhibit 17); Dep. Tr. of J. Maxey, Southeast Urology Network Designee (Jan. 17, 2014) at 78-79 (stating that, except in limited circumstances, patient would not know which lab was testing their specimen and patient would not know about lab’s data security practices before specimen was sent) (attached as Exhibit 18); Dep. Tr. of L. Randolph, Midtown Urology Designee (Feb. 4, 2014) at 66-67 (stating that great majority of patients did not know their specimen was going to LabMD and patient would not know about LabMD’s data security practices) (attached as Exhibit 19).

Peer-to-Peer File Sharing Application

12. P2P applications allow a user to both designate files on the user’s computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network. Ans. ¶ 14 (Ex. 1); Expert Report of Clay Shields, Ph.D. (“Shields Report”) ¶¶ 14, 17-18, 22, 29, 31, 56-57, 65, 69-71 (attached as Exhibit 20).

13. After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. Generally, once shared, a file cannot with certainty be removed permanently from a P2P network. Ans. ¶ 15 (Ex. 1); Shields Report ¶ 21 (Ex. 20); Hill Report ¶ 44 (Ex. 2).

14. Since at least 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. Ans. ¶ 16 (Ex. 1); Shields Report ¶¶ 40-48 (Ex. 20) (identifying the research literature); FTC Consumer Alert: File-Sharing: A Fair Share? Maybe Not (July 2003) (attached as Exhibit 21); Revised FTC Consumer Alert: P2P File-Sharing: Evaluating the Risks (June 2005) (attached as Exhibit 22); Revised FTC Consumer Alert: P2P File-Sharing: Evaluate the Risks (July 2005) (attached as Exhibit 23); FTC Distribution: Revised P2P File Sharing: Evaluate the Risks (Dec. 2006) (attached as Exhibit 24); FTC Distribution: Revised P2P File Sharing: Evaluate the Risks (Feb. 2008) (attached as Exhibit 25); Revised FTC Spanish Consumer Alert: File-Sharing: Evaluating the Risks (Spanish July 2005) (attached as Exhibit 26); Revised FTC Spanish Consumer Alert: File-Sharing: Evaluating the Risks (Spanish Oct. 2006) (attached as Exhibit 27); Revised FTC Spanish Consumer Alert: File-Sharing: Evaluate the Risks (Spanish Feb. 2008) (attached as Exhibit 28).

Security Incidents

15. After receiving the May 2008 notice that the P2P insurance aging file was available through LimeWire, Respondent determined that at that point in time, the P2P insurance aging file was one of hundreds of files that were designated for sharing from the billing computer using LimeWire. Ans. ¶ 18(b) (Ex. 1) (denying that the P2P insurance aging file was designated for sharing); FTC-LABMD-003755 (screenshot produced by LabMD of billing computer showing that more than 900 files were being shared on the P2P network through LimeWire, including the P2P insurance aging file, listed as "insuranceaging_6.05.071.pdf") (attached as Exhibit 29); Simmons Dep. Tr. at 36-39 (stating that "insuranceaging_6.05.071.pdf" is the P2P insurance aging file found by Tiversa) (Ex. 16).

16. In October 2012, the Sacramento, California Police Department found more than 35 Day Sheets and a small number of copied checks in the possession of individuals who pleaded no contest to state charges of identity theft. Ans. ¶ 21 (Ex. 1); Dep. Tr. of K. Jestes (Dec. 17, 2013) at 22-23, 43-44 (attached as Exhibit 30); Sup. Ct. of Cal.: Erick Garcia Minute Order re Plea (attached as Exhibit 31); Sup. Ct. of Cal.: Josie Martinez Maldanado Minute Order re Plea (attached as Exhibit 32).

17. A number of the Social Security numbers in the Day Sheets are being, or have been, used by people with different names, which may indicate that the Social Security numbers have been used by identity thieves. Ans. ¶ 21 (Ex. 1); Kam Report at 23 (Ex. 17).

Consumer Injury

18. LabMD's security practices caused or are likely to cause substantial injury to consumers. Ans. ¶ 22 (Ex. 1); Kam Report at 8-10, 17-23 (Ex. 17).

PART II: COMPLAINT COUNSEL'S RESPONSE TO RESPONDENT'S STATEMENT OF "UNDISPUTED FACTS"

Pursuant to Rule 3.24, Complaint Counsel responds to several of the facts Respondent LabMD contends are "undisputed" in its Motion for Summary Decision, and in so doing demonstrates that there are numerous material factual issues as to which there is a genuine issue for the evidentiary hearing. 16 C.F.R. § 3.24. Complaint Counsel reserves the right to introduce evidence and testimony at the evidentiary hearing to contest each fact set forth in Respondent's Motion for Summary Decision even if not contested for the purposes of Complaint Counsel's Opposition to Respondent's Motion for Summary Decision.

1. *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.*

Complaint Counsel's Response: Not supported by evidence, and irrelevant and immaterial.

Respondent cites no evidence to support its contention that LabMD is a "Covered Entity." Whether LabMD "receives, maintains and transmits PHI during the normal course of business" is neither relevant nor material to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA, HITECH, or their implementing regulations, and Respondent did not raise HIPAA, HITECH, or their implementing regulations as an affirmative defense. *See* Ans. at 6-7.

2. *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.*

Complaint Counsel's Response: Misleading, not supported by evidence, and irrelevant and immaterial.

Complaint Counsel disputes the use of the term "took possession." Tiversa downloaded a copy of the Insurance Aging File on a P2P network. Resp. Mot. Summ. Dec. at Ex. 1. It did not "take possession" of the file to the extent this implies that it obtained the file directly from LabMD or obtained exclusive ownership of the file.

The evidence Respondent cites to support this contention is insufficient. *See* Resp. Mot. Summ. Dec. at Ex. 1. Respondent's exhibit does not establish that the file was downloaded without LabMD's knowledge or consent, does not establish that Tiversa "took possession" of the file, and does not state that this event took place on February 5, 2008. *Id.*

Even if undisputed, this contention is neither relevant nor material to Respondent's request for summary decision. To be material the fact must "affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby*, 477 U.S. 242, 248 (1986). Respondent's contention regarding Tiversa and the Insurance Aging File supports Complaint Counsel's allegations that Respondent's data security practices caused or are likely to cause substantial consumer injury that consumers could not reasonably avoid and is not outweighed by countervailing benefits to consumers or competition.

3. *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.*

Complaint Counsel's Response: Misleading, not supported by evidence, and irrelevant and immaterial.

Respondent cites no evidence to support its contention that Tiversa made the Insurance Aging File available to Professor Johnson. *See* Resp. Mot. Summ. Dec. at Ex. 2. This evidence merely states that "[e]xperiments conducted in this paper were conducted in collaboration with Tiversa . . ." *Id.* Even if undisputed, this contention is neither relevant nor material to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

4. *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.*

Complaint Counsel's Response: Not supported by evidence, and irrelevant and immaterial.

Respondent cites no evidence to support its contentions that the FTC began its investigation in January 2010 and that the investigation was based on the disclosure of PHI. Even if undisputed, these contentions are neither relevant nor material to Respondent's request for summary decision. The Commission's bases for issuing the Complaint is not an issue to be determined in this proceeding. *See, e.g.*, Order on Complaint Counsel's Motion to Quash Subpoena Served on Complaint Counsel and for Protective Order (Jan. 30, 2014), at 6 ("Precedent dictates that [the bases for the Commission's commencement of this action] are not relevant . . . in an administrative adjudication.").

5. *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.*

Complaint Counsel's Response: Not supported by evidence, and irrelevant and immaterial.

Respondent cites no evidence to support its contention that Detective Jestes, or anyone else with the Sacramento police, "googled" LabMD and discovered that LabMD was "under investigation by the FTC." Detective Jestes' testimony cited to by Respondent and provided as an exhibit simply states that she "looked and saw that none of [the consumers' whose information was in the documents found by the Sacramento Police] had a Sacramento connection based on their information on the checks, and [that she] may have done a simple Google-type search to see if they had a connection [to Sacramento]. . . ." *See* Resp. Mot. Summ. Dec. at Ex. 3.

This contention, even if not disputed, is irrelevant to this case because the actions of the Sacramento Police have no bearing on the reasonableness of LabMD's data security practices and do not relate to any of Respondent's affirmative defenses. Ans. at 6-7. Even if relevant, which it is not, this contention is immaterial to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

6. *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.*

Complaint Counsel's Response: Not supported by evidence, and irrelevant and immaterial.

Respondent cites no evidence to support its contention that the Sacramento Police notified the FTC that it had discovered LabMD documents, that the Sacramento Police did not notify LabMD of its finding the documents, or that the Sacramento Police had any awareness as to LabMD's "duty to notify under HIPAA" and to whom that obligation would relate. *See* Resp. Mot. Summ. Dec. at Ex. 3. The testimony to which Respondent cites has been completely redacted, and no testimony in the following excerpted pages supports Respondent's statement. *Id.*

Even if this contention were undisputed by Complaint Counsel, it is neither relevant nor material to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

7. *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).*

Complaint Counsel's Response: Not a statement of fact, not supported by evidence, and irrelevant and immaterial.

This statement is a legal conclusion. Respondent cites no evidence to support its assertion that that LabMD is a HIPAA-covered entity that must comply with specific regulations.

Even if undisputed, this assertion is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA, HITECH, or their implementing regulations, and Respondent did not raise HIPAA, HITECH, or their implementing regulations as an affirmative defense in its Answer. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

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

Complaint Counsel's Response: Not supported by evidence, and irrelevant and immaterial.

This statement is a legal conclusion. Respondent cites no evidence to support its assertion that the HIPAA Security Rule has data security standards or that LabMD is a HIPAA-covered entity that must comply with specific data security standards.

Even if characterized as an undisputed fact, the assertion is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to the HIPAA Security Rule, and Respondent did not raise the HIPAA Security Rule as an affirmative defense. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

9. *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….").*

Complaint Counsel's Response: Not a statement of fact, not supported by evidence, and irrelevant and immaterial.

This statement is a legal conclusion. Whether HHS exclusively enforces HIPAA and HITECH is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA or HITECH, and Respondent did not raise HIPAA or HITECH as an affirmative defense in its Answer. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

10. *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.*

Complaint Counsel's Response: Irrelevant and immaterial.

This contention is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA, HITECH, or their implementing regulations, and Respondent did not raise HIPAA, HITECH, or their implementing regulations as an affirmative defense in its Answer. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

11. *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.*

Complaint Counsel's Response: Not supported by evidence, irrelevant and immaterial.

Complaint Counsel disputes this contention. The Commission "has repeatedly affirmed its authority to take action against unreasonable data security measures as 'unfair . . . acts or practices' in violation of Section 5." MTD Order at 8. Complaint Counsel sets forth in ¶¶ 1 through 18 of Part I of this statement the disputed facts Complaint Counsel intends to establish at trial to show that LabMD failed to provide reasonable data security.

Even if undisputed, which it is not, this contention does not support Respondent's request for summary decision, as it is irrelevant and immaterial. *See Anderson*, 477 U.S. at 248.

12. *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.*

Complaint Counsel's Response: Irrelevant and immaterial.

Respondent's contention regarding Complaint Counsel's statement relating to pleading requirements under the FTC Act is irrelevant and immaterial to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

13. *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.*

Complaint Counsel's Response: Irrelevant and immaterial.

Respondent's contentions regarding Complaint Counsel's answers to questions about sources of information regarding data security are irrelevant and immaterial to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

14. *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.*

Complaint Counsel's Response: Misleading, not supported by evidence, irrelevant and immaterial.

Complaint Counsel disputes this contention. Complaint Counsel has produced to Respondent Commission business publications, consumer publications, Congressional testimony, consent orders, speeches, and other material that has been made available to businesses and the public as guidance on reasonable data security. *See, e.g.*, FTC Facts for Business, Security Check: Reducing Risks to your Computer Systems (June 2003) (attached as Exhibit 33);

Protecting Information Security and Preventing Identity Theft, Prepared Statement of the FTC before Subcomm. on Tech., Info. Policy, Intergov't Relations, and Census, Comm. On Gov't Reform, U.S. House of Representatives. (Sept. 22, 2004) (attached as Exhibit 34); *In re The TJX Cos.*, FTC Dkt. No. C-4227, FTC File No. 072-3055 (July 29, 2008) (attached as Exhibit 35).

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.*

Complaint Counsel's Response: Irrelevant and immaterial.

Respondent's contentions regarding Complaint Counsel's answers to questions about sources of information regarding data security are irrelevant and immaterial to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

16. *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.*

Complaint Counsel's Response: Irrelevant and immaterial.

Respondent's characterization of Complaint Counsel's responses to Respondent's discovery requests is irrelevant and immaterial to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

17. *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.*

Complaint Counsel's Response: Irrelevant and immaterial.

Respondent's contention regarding Complaint Counsel's response to a question about rules or regulations not pled in the Complaint is irrelevant and immaterial to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

18. *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.*

Complaint Counsel's Response: Irrelevant and immaterial.

Respondent's contentions regarding the allegations in the Complaint and the relief sought in the notice order are irrelevant and immaterial to Respondent's request for summary decision. *See Anderson,* 477 U.S. at 248.

Dated: May 7, 2014

Respectfully submitted,

Megan Cox

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

Federal Trade Commission
600 Pennsylvania Avenue, NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-2282 – Cox
Facsimile: (202) 326-3062
Electronic mail: mcox1@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on May 7, 2014, I filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system.

I also certify that I caused twelve (12) copies of the foregoing document to be delivered to the Office of the Secretary, Room H-113.

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

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

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

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

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

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

CERTIFICATE FOR ELECTRONIC FILING

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

May 7, 2014

By: Megan Cox
Megan Cox
Federal Trade Commission
Bureau of Consumer Protection

EXHIBIT 1

PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
09 17 2013
566807
SECRETARY

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. 9357

PUBLIC DOCUMENT

RESPONDENT LABMD, INC.'S ANSWER AND DEFENSES TO ADMINISTRATIVE COMPLAINT

Pursuant to 16 C.F.R. § 3.12(b), Respondent LabMD, Inc. ("LabMD"), respectfully submits the following Answer and Defenses to the allegations of the Complaint issued by the Federal Trade Commission ("Commission") on August 28, 2013. Except to the extent specifically admitted herein, LabMD denies each and every allegation in the Complaint, including all allegations contained in headings or otherwise not contained in one of the Complaint's 23 numbered paragraphs. Specifically, LabMD denies that it has engaged in conduct that violates Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and denies that this proceeding is in any way in the public interest.

RESPONDENT'S BUSINESS

1. Admitted.

2. Denied to the extent legal conclusions require an answer.

3. LabMD admits that it is a clinical laboratory that conducts laboratory tests on specimen samples and reports test results to authorized physicians since at least 2001. The balance of the averment is denied.

Exhibit 1

4. LabMD admits that it files insurance claims for charges related to the clinical laboratory tests with health insurance companies. LabMD admits that insured referring physicians' patients may pay the part of LabMD's charges not covered by insurance and that uninsured referring physicians' patients may be responsible for the full amount of the charges in some instances. LabMD is without knowledge and information sufficient to form a belief as to whether referring physicians' patients in many instances pay with credit cards or personal checks, as "many" and "typically" are highly subjective terms, and therefore denies that allegation. LabMD denies the balance of the averment.

5. LabMD admits that it currently tests samples from referring physicians' patients in Georgia, which may be sent from six states outside of Georgia: Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona. LabMD denies the balance of the averment.

6. LabMD admits that, as a clinical laboratory that conducts laboratory tests and files insurance claims for charges related to the clinical laboratory tests with health insurance companies, LabMD may be provided with the following information about referring physicians' patients: names; addresses; dates of birth; gender; telephone numbers; Social Security numbers ("SSN"); referring health care provider names, addresses, and telephone numbers; laboratory tests and test codes; and health insurance company names and policy numbers. The balance of the averment is denied.

7. Denied.

8. LabMD admits that it currently has a computer network and uses a computer network in conducting its business. LabMD denies that it operates computer networks. The balance of the averment is vague and unclear and so it is denied.

9. LabMD admits that it currently uses a computer network to receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to referring physicians' patients; and prepare medical records. LabMD denies that it currently uses computer networks to obtain approvals for payments made by referring physicians' patients with credit cards. LabMD admits that LabMD's billing department currently accesses documents related to processing claims and payments using computers that are nodes of a computer network. The balance of the averment is vague and unclear and so it is denied.

(a) LabMD admits that LabMD's billing department currently generates spreadsheets of insurance claims and payments, which may include information such as referring physicians' patients' names, dates of birth, and SSNs; the American Medical Association current procedural terminology ("CPT") codes for the laboratory tests conducted; and health insurance company names, addresses, and policy numbers. The balance of the averment is denied.

(b) LabMD admits that LabMD's billing department currently uses computers to create spreadsheets of payments received from referring physicians' patients ("Day Sheets"), which may include personal information such as referring physicians' patients' names; SSNs; and methods, amounts, and dates of payments. The balance of the averment is denied.

(c) Denied.

RESPONDENT'S SECURITY PRACTICES

10. Denied.

11. Denied.

Exhibit 1

12. LabMD lacks knowledge and information sufficient to form a belief as to the truth or falsity of the averment so it is denied.

PEER-TO-PEER FILE SHARING APPLICATIONS

13. Admitted.

14. LabMD lacks knowledge and information sufficient to form a belief as to whether peer-to-peer ("P2P") users can "designate files on the user's computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network," as it is unclear what is meant by "designate files," "designated files," "available," and "P2P network," and therefore denies the averment.

15. LabMD lacks information and knowledge sufficient to form a belief as to the truth or falsity of the averment so it is denied.

16. LabMD lacks information and knowledge sufficient to form a belief as to the truth or falsity of the averment so it is denied.

SECURITY INCIDENTS

17. LabMD admits that a third party, Tiversa, Inc. ("Tiversa"), contacted LabMD in May 2008 and claimed to have obtained a June 2007 insurance aging report from LabMD via Limewire, a P2P file sharing application. The balance of the averment is denied.

18. LabMD lacks knowledge and information sufficient to form a belief as to whether the "P2P insurance aging file" was "available" on Limewire. LabMD admits that Tiversa claimed that the "P2P insurance aging file" could be obtained via Limewire in May 2008. LabMD denies the balance of the averment.

Exhibit 1

(a) LabMD admits that it believes that Limewire had been downloaded and installed on a computer used by LabMD's billing department manager but denies the balance of the averment.

(b) LabMD admits that hundreds of music files were found on the billing computer and could be shared using Limewire. LabMD does not have information and knowledge sufficient to form a belief as to the truth or falsity of the allegations that the "P2P insurance aging file" and other files in the billing computer were "designated for sharing" and therefore denies the balance of the averment.

(c) LabMD admits that it believes that a version of Limewire may have been installed on the billing computer no later than 2006. LabMD lacks knowledge and information sufficient to form a belief as to the truth or falsity of the balance of the averment so it is denied.

19. LabMD admits that the P2P insurance aging file contained personal information about approximately 9,300 referring physicians' patients, including names, dates of birth, SSNs, CPT codes, and health insurance company names, addresses, and policy numbers. The balance of the averment is denied.

20. Admitted.

21. LabMD lacks information and knowledge sufficient to form a belief as to the truth or falsity of the averment so it is denied.

VIOLATION OF THE FTC ACT

22. Denied.

23. Denied.

Exhibit 1

DEFENSES

Without assuming any burden of proof that it would not otherwise bear, and reserving the right to assert additional defenses as this matter proceeds, pursuant to 16 C.F.R. § 3.12(b)(1)(i), LabMD asserts the following defenses:

FIRST DEFENSE

The Complaint fails to state a claim upon which relief can be granted.

SECOND DEFENSE

The Commission is without subject-matter jurisdiction over the claims asserted in this case.

THIRD DEFENSE

Section 5 of the FTC Act does not give the Commission the statutory authority to regulate the acts or practices alleged in the Complaint and therefore the Commission's actions are arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; contrary to constitutional right, power, privilege, or immunity; in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; or without observance of procedure required by law.

FOURTH DEFENSE

The acts or practices alleged in the Complaint do not cause, and are not likely to cause, substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition, as required by 15 U.S.C. § 45(n), and therefore the Commission has no authority under Section 5 of the FTC Act to declare unlawful the acts or practices alleged in the Complaint.

Exhibit 1

FIFTH DEFENSE

Even if the Commission had subject-matter jurisdiction over the claims asserted in this case, which it does not, because the Commission has not published any rules, regulations, or other guidelines clarifying and providing any notice, let alone constitutionally adequate notice, of what data-security practices the Commission believes Section 5 of the FTC Act forbids or requires and has not otherwise established any meaningful standards, this enforcement action against LabMD violates the due process requirements of fair notice and appropriate standards for enforcement guaranteed and protected by the Fifth Amendment to the U.S. Constitution and the Administrative Procedure Act.

CONCLUSION

WHEREFORE, LabMD respectfully requests that the Administrative Law Judge deny the Commission's requested relief and dismiss the Complaint in its entirety with prejudice.

Respectfully submitted,

/s/ Reed Rubinstein
Reed D. Rubinstein
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: (202) 372-9120
Fax: (202) 372-9141
reed.rubinstein@dinsmore.com

/s/ Michael D. Pepson
Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.2024
Fax: 202.330.5842
michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Dated: September 17, 2013

Exhibit 1

PUBLIC

CERTIFICATE OF SERVICE

I hereby certify that on September 17, 2013, 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 also certify that I delivered via electronic mail and first-class mail 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
Megan Cox
Margaret Lassack
Ryan Mehm
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE FOR ELECTRONIC FILING

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

Dated: September 17, 2013 By: /s/ Michael D. Pepson

Exhibit 1

Exhibit 2

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.

Exhibit 2

TABLE OF CONTENTS

Exhibit 2

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.

Exhibit 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

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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

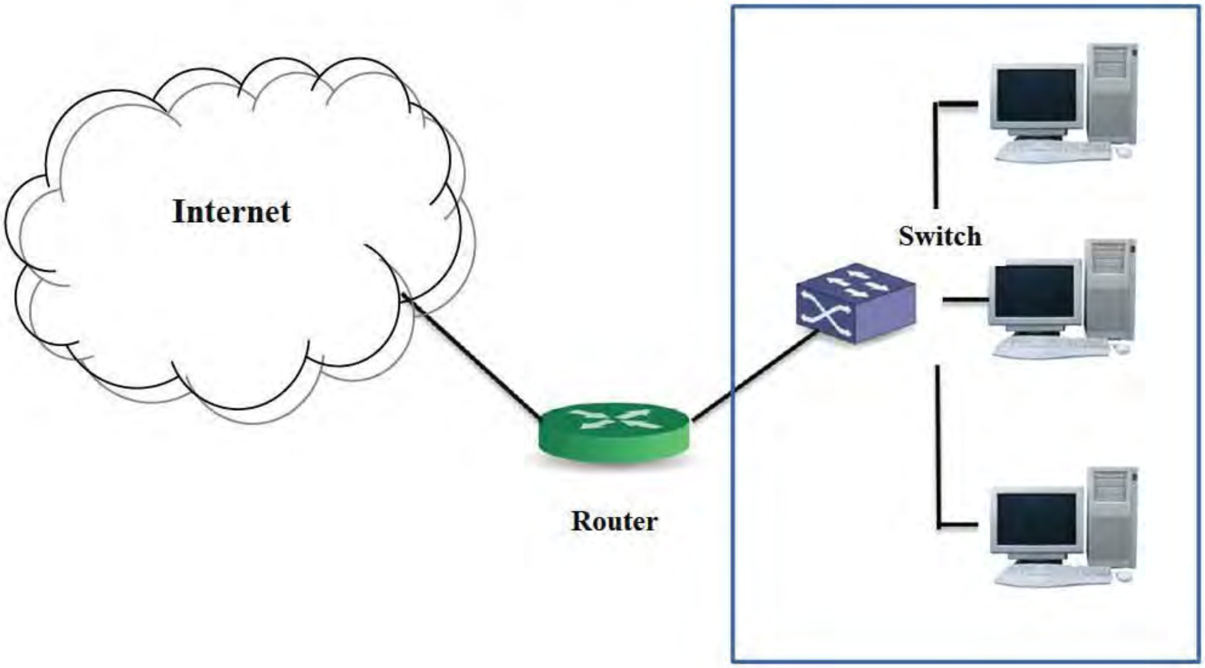


Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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

Exhibit 2

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

Exhibit 2

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.

Exhibit 2

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

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

c. **<u>Ports</u>:** 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. **<u>Policies</u>:** 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.

Exhibit 2

    - 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. **Protect:** 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. **Probe:** 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.

Exhibit 2

g. **<u>Physical</u>:** 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

Exhibit 2

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).

Exhibit 2

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).

Exhibit 2

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. <u>Paragraph 10</u>: "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

Exhibit 2

that the systems would be 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,

Exhibit 2

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).

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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

Exhibit 2

(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.

Exhibit 2

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).

Exhibit 2

- 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.

Exhibit 2

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.

Exhibit 2

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).

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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

Exhibit 2

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.

Exhibit 2

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

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

- 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.

Exhibit 2

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).

Exhibit 2

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."

Exhibit 2

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).

Exhibit 2

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.

Exhibit 2

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

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

Appendix A

Exhibit 2

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/~ralhill

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

Exhibit 2

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).

Exhibit 2

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.

Exhibit 2

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.

Exhibit 2

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.

.

Exhibit 2

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.

Exhibit 2

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

Exhibit 2

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**

Exhibit 2

Appendix B

Exhibit 2

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

Exhibit 2

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

<u>Documents Produced by LabMD</u>

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

Exhibit 2

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

<u>Documents Produced by Tiversa</u>
TIVERSA-FTC RESPONSE-000001-006904

<u>Documents Produced by Sacramento Police Department</u>
FTC-SAC-000001-FTC-LABMD-000044

<u>Documents Produced by the Privacy Institute</u>
FTC-PRI-000001-FTC-PRI-001719

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

Exhibit 2

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.

Exhibit 2

- 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.

Exhibit 2

- 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.

Exhibit 2

- 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).

Exhibit 2

- 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 2

EXHIBIT 3

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

REBUTTAL EXPERT REPORT OF RAQUEL HILL, PH.D.

I. Introduction

1. I am Dr. Raquel Hill, a tenured professor of Computer Science at Indiana University. I have over 25 years of combined academic, research, and industrial experience in computing, with expertise in computer security, data privacy, and networking systems. I submitted an Expert Report on behalf of Complaint Counsel in this matter on March 18, 2014 (Initial Expert Report).[1]

2. I have been asked by Complaint Counsel to evaluate and comment on the Expert Report of Adam Fisk submitted on behalf of LabMD in this matter (Fisk Report), specifically Mr. Fisk's rebuttal to my Initial Expert Report and his opinions regarding LabMD's network security practices.

3. I discussed my experience and qualifications as an expert in Section II of my Initial Expert Report and attached a copy of my *curriculum vitae* as Appendix A to my Initial Expert Report. In reaching my conclusions, I considered the Fisk Report and some of the materials cited

[1] See Expert Report of Raquel Hill, Ph.D., In the Matter of LabMD, Inc., Docket No. 9357, dated March 18, 2014 (CX0740) (Initial Expert Report).

Exhibit 3

therein, materials listed in Appendix B to my Initial Expert Report, and the materials listed in Appendix A to this report.[2]

4. Based upon my review of these materials and my experience described in Section II of my Initial Expert Report, I conclude that Mr. Fisk's opinion that "LabMD's security was reasonable and adequate"[3] to protect the Personal Information[4] maintained on its network during the Relevant Time Period[5] is unreliable and fundamentally flawed because:

a. As I explain in Section II, below, Mr. Fisk's analysis of the adequacy of LabMD's security practices fails to address the goals, policies, and mechanisms of a comprehensive information security program that implements a defense in depth strategy; and

b. As I explain in Sections III and IV, below, Mr. Fisk's analysis of the adequacy of LabMD's security practices is not supported by the record evidence.

5. Nothing in the Fisk Report changes my conclusion that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network,[6] or the opinions that I provided in my Initial Expert Report in support of that conclusion.

[2] I reserve the right to revise or supplement my opinions based upon 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.

[3] Fisk Report, p. 34.

[4] "Personal Information" has the same meaning in this report as in my Initial Expert Report. See Initial Expert Report, ¶ 2, n.1 (citing Complaint Counsel's February 19, 2014 Requests for Admission to LabMD, p. 2).

[5] As I explained in Paragraphs 4 and 48 of my Initial Expert Report, the Relevant Time Period is January 2005 through July 2010.

[6] See Initial Expert Report, ¶ 4.

Exhibit 3

II. Mr. Fisk's Analysis of the Adequacy of LabMD's Security Practices is Unreliable

6. Mr. Fisk's analysis of the adequacy of LabMD's security practices during the Relevant Time Period is unreliable because he fails to address the goals, policies, and mechanisms of a comprehensive information security program that implements a defense in depth strategy.

7. Defense in depth is the most effective way to provide reasonable security for a network, its computers, and the information that it stores. Implementing an appropriate defense in depth strategy requires more than the deployment of technical measures, such as firewalls. It requires that an organization identify the resources that are to be protected, specify an appropriate set of security goals and policies for protecting those resources, and deploy mechanisms that are appropriately configured to enforce those policies. Simply deploying security mechanisms without going through the process of developing a comprehensive set of goals and policies for protecting a network generally does not result in defense in depth.[7] When an organization fails to develop a comprehensive information security program, it sets itself up to fail at protecting its critical and sensitive resources.

8. Mr. Fisk fails to explain how LabMD integrated security goals, policies, and mechanisms into a comprehensive information security program that implements a defense in depth strategy. As I explained in my Initial Expert Report, an organization should implement a defense in depth strategy that deploys multiple security measures at each layer of the network to address the myriad risks that an organization faces and reduce the overall likelihood that an attack will succeed or an unauthorized disclosure will occur.[8]

[7] See Initial Expert Report, ¶¶ 27-31, 52.

[8] See Initial Expert Report, ¶¶ 27-31.

Exhibit 3

9. An appropriate defense in depth strategy must be driven not just by the size of the organization, but by the resources that the organization needs to protect. For LabMD, those resources include large amounts of highly sensitive Personal Information, including Social Security numbers, medical insurance information, and medical diagnosis codes. As I explained in my Initial Expert Report, the more sensitive the Personal Information maintained within the network, the greater the need for enhanced security measures to provide reasonable and appropriate security.[9]

10. The record shows that LabMD did not specify security goals or policies that were sufficiently comprehensive to protect the large amounts of sensitive Personal Information maintained on its network during the Relevant Time Period.[10] Because LabMD did not have such a roadmap for selecting and deploying security measures, it deployed technical security measures in an ad hoc manner, as the record shows.[11] This left LabMD vulnerable to known or reasonably foreseeable threats that could have been mitigated through goal-oriented security measures such as risk assessments, the application of software updates, and employee training.

11. Although Mr. Fisk does not dispute the importance of defense in depth, he fails to address whether LabMD implemented a defense in depth strategy. Instead he focuses his analysis primarily on one type of technical security measure—LabMD's firewalls—which he contends adequately protected LabMD's network.[12] Because Mr. Fisk's analysis fails to address the goals, policies, and mechanisms of a comprehensive information security program implementing a

[9] See Initial Expert Report, ¶¶ 74-75.

[10] See Initial Expert Report, ¶ 61.

[11] See Initial Expert Report, ¶ 91.

[12] Mr. Fisk also discusses several other LabMD security practices in his analysis. See, for example, Fisk Report, pp. 16-23, 33-34. As I explain in Section IV, below, Mr. Fisk's contentions about these practices are not supported by the record.

Exhibit 3

defense in depth strategy, his conclusion that LabMD's security practices were reasonable and appropriate is unreliable.

12. As Mr. Fisk's critique of my analysis indicates, firewalls alone are not sufficient to protect a network against certain known and reasonably foreseeable threats, such as LimeWire. Mr. Fisk acknowledges that LimeWire was designed to allow files to be shared even if the computer sharing files is behind a firewall that blocks incoming connection requests. This illustrates the importance of defense in depth, because a single technical security measure, such as a firewall, does not protect against this risk or other threats that are designed to evade that technical security measure.

13. The fact that LimeWire was designed to evade firewall settings[13] affects only two examples in support of my opinion that LabMD did not employ readily available measures to prevent or detect unauthorized access to its network. I provided a number of other examples in support of that opinion,[14] and as I explain in Paragraph 19 below, there is additional evidence in the record that LabMD's firewalls were not properly configured to block certain known and reasonably foreseeable threats. Therefore, the fact that LimeWire can evade firewall settings does not affect that opinion. It also does not affect my conclusion that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, or my other opinions in support of that conclusion.[15]

[13] See Fisk Report, pp. 26-28.

[14] See Initial Expert Report, ¶¶ 102-106.

[15] See Initial Expert Report, ¶ 4. Mr. Fisk also critiques my analysis of the risk of Windows shared folders. Although he is correct that LimeWire does not automatically present the contents of Windows shared folders to other LimeWire users as information that is available to be downloaded, that does not affect my analysis regarding the other risks associated with the use of Windows shared folders or my opinion that employees should not be permitted to create Windows shared folders on their workstations. See Initial Expert Report, ¶ 104(d).

Exhibit 3

III. Mr. Fisk's Opinions about the Configuration of LabMD's Firewalls and Router Are Not Supported by the Record Evidence

14. Not only is Mr. Fisk's analysis of the adequacy of LabMD's security practices unreliable because it fails to address the goals, policies, and mechanisms of a comprehensive information security program implementing a defense in depth strategy, as I explained in Section II above, but it is also not supported by the record evidence. Specifically, the record does not support Mr. Fisk's opinions about the configuration of LabMD's firewalls and router, including his opinion that LabMD's firewalls were configured to block all incoming connections.

15. Mr. Fisk contends that LabMD's firewalls were configured by default to block all connections that originated outside of LabMD's network.[16] He then assumes that LabMD used these default configurations throughout the Relevant Time Period.[17] This assumption is fundamentally flawed because, had the LabMD firewalls been configured to block all incoming connections as Mr. Fisk assumes, LabMD would not have been able to conduct its business.

16. The default configurations of LabMD's firewalls were not designed to meet the specific communications needs of LabMD. For LabMD to conduct business, its firewalls had to be configured to allow some incoming connections. For example, the firewalls had to be configured to allow LabMD physician clients to initiate connections from outside of LabMD's network in order to transfer patient Personal Information to LabMD via File Transfer Protocol (FTP) transfer or through LabMD's web-based application interface.[18] If Mr. Fisk's assumption about the configuration of LabMD's firewalls were correct, LabMD's firewalls would have blocked these connections, and the patient Personal Information would not have been transferred to

[16] See, for example, Fisk Report, p. 20.

[17] See, for example, Fisk Report, p. 26.

[18] For a description of how LabMD's physician clients transferred patients' Personal Information to LabMD, see Initial Expert Report, ¶¶ 33-35.

Exhibit 3

LabMD. However, the record shows that patient Personal Information was transferred to LabMD throughout the Relevant Time Period.[19]

17. The default firewall configurations that Mr. Fisk contends were in place would have also prevented LabMD's remote employees from accessing the network,[20] blocked LabMD's incoming email traffic,[21] and possibly prevented LabMD from receiving lab results from tests that it outsourced to certain other laboratories.[22]

18. Record evidence confirms that LabMD changed the default firewall settings during the Relevant Time Period. For example, an invoice from LabMD contractor APT shows that, on June 1, 2006, APT changed the firewall settings to allow individuals from outside of the network to access one or more LabMD applications. The invoice states: "Worked with Pat on setting up the second firewall and making sure people were able to get to the application from outside the network."[23]

[19] See, for example, LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 17; Michael Daugherty March 4, 2014 Deposition Transcript, pp. 138-139; Michael Daugherty February 10, 2014 Deposition Transcript, p. 131.

[20] The record shows that LabMD employees accessed the LabMD network remotely. See, for example, Sandra Brown January 11, 2014 Deposition Transcript, pp. 9-13; Jennifer Parr February 11, 2014 Deposition Transcript, p. 40; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 239-240. See also Initial Expert Report, ¶ 40.

[21] The record shows that LabMD maintained its own email server, which was located on its network. See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, p. 163; Jennifer Parr February 11, 2014 Deposition Transcript, pp. 44-47; FTC-LABMD-000002 through FTC-LABMD-000003 (CX0034); FTC-LABMD-003646 (CX0039).

[22] The record shows that LabMD received lab results from other laboratories via Virtual Private Network (VPN) connections with those laboratories. See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 100; FTC-PVD-000054 (CX0052) (Final Page of ProviDyn Service Solutions Proposal listing name and Public IP Addresses for network security scans); FTC-PVD-001186 through FTC-PVD-001210 (CX0074) (May 2010 Scan of LabCorp VPN).

[23] See FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035), p. 3.

Exhibit 3

19. Mr. Fisk also contends that “[t]here is no evidence that LabMD’s firewalls were in fact misconfigured.”[24] Contrary to his assertion, there is evidence in the record indicating that LabMD’s firewalls were not properly configured to block certain known and reasonably foreseeable threats to LabMD’s network. For example, the external vulnerability scans that ProviDyn conducted in May 2010 indicate that port 10,000 was open.[25] The application that used that port was LabMD’s Veritas backup application, which did not need to be accessed by individuals who were outside of LabMD’s network. Therefore, there was no business need for port 10,000 to be open. Furthermore, Symantec issued an alert in 2005 recommending that port 10,000 be closed until the Veritas backup application was updated to correct a significant vulnerability.[26] The ProviDyn external vulnerability scans show that not only was port 10,000 open in 2010, but also that LabMD’s Veritas backup application had not been updated to correct the vulnerability that Symantec identified.[27] Updating applications is an important part of reasonable and appropriate security.[28]

20. Mr. Fisk also speculates that Cypress may have enabled any intrusion detection and prevention capabilities that LabMD’s Cisco 1841 router had. There is no evidence in the record that is the case. To the contrary, testimony from several former LabMD employees indicates that LabMD had neither an intrusion detection system (IDS) nor an intrusion prevention system (IPS)

[24] See Fisk Report, p. 34.

[25] See FTC-PVD-000865 through FTC-PVD-000934 (CX0067).

[26] See 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 April 11, 2014.

[27] See FTC-PVD-000865 through FTC-PVD-000934 (CX0067).

[28] See Initial Expert Report, ¶ 31.

Exhibit 3

in place during the Relevant Time Period.[29] In addition, there is no evidence in the record of logs or other alerts that normally would have been created by an IDS or an IPS.

IV. Mr. Fisk's Opinion that LabMD's Network "Adhered to Best Practices" Is Not Supported by the Record Evidence

21. In addition to his claims about the configuration of LabMD's firewalls and router (which are not supported by the record, as I explained in Section III, above), Mr. Fisk makes three other claims in support of his opinion that "LabMD's network adhered to best practices during the Relevant Time Period": (1) LabMD outsourced its network infrastructure to Cypress and APT, and "there is no evidence that those firms did not deploy secure networks using best practices" (Cypress/APT Claim); [30] (2) Starting in 2001, LabMD had an "Employee User Account Policy" that prohibited downloading and "installing applications that were unnecessary for performing work duties" (Employee User Account Policy Claim);[31] and (3) LabMD attempted to detect unauthorized applications by performing manual inspections that Mr. Fisk implies were as effective, but less efficient, than an automated File Integrity Monitor (Manual Inspection Claim).[32] As I explain below, none of these claims is supported by the evidence in the record.

A. Cypress/APT Claim

22. The record evidence does not support Mr. Fisk's Cypress/APT Claim. Rather, the evidence in the record indicates that Cypress was a passive ISP and that LabMD had

[29] See, for example, Allen Truett February 27, 2014 Deposition Transcript, p. 122; Robert Hyer December 13, 2013 Deposition Transcript, pp. 123-124, 126; Patrick Howard January 24, 2014 Deposition Transcript, pp. 58, 140; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 92.

[30] Fisk Report, p. 33.

[31] Fisk Report, pp. 22-23, 33.

[32] Fisk Report, p. 33.

Exhibit 3

responsibility for the security of its network.[33] For example, Cypress designee Peter Sandrev testified that Cypress provided LabMD a "highway to get to and from the internet" and nothing more, and that LabMD has responsibility for the security and management of its information.[34]

23. The record also indicates that the only security measures that APT deployed were: (1) one or more firewalls, which did not have IDS or IPS features enabled, and (2) antivirus software. Furthermore, the evidence shows that APT did not actively monitor the operation of LabMD's firewalls, but rather monitored their operation only in an "ad hoc" way when responding to problems raised by LabMD employees.[35]

24. In addition, the record indicates that, by 2007, LabMD had started to use its own IT employees, headed by Curt Kaloustian, as a replacement for APT's services.[36] If Mr. Fisk is correct that Mr. Kaloustian had a "limited understanding of computer networks," this is additional evidence that LabMD's network was not managed using "best practices" as Mr. Fisk contends. Mr. Kaloustian, as LabMD's lead IT employee, had first-hand knowledge about LabMD's network and practices during much of the Relevant Time Period. Accordingly, in forming my opinions, I credited testimony from Mr. Kaloustian that describes LabMD's practices and network setup during his tenure.

[33] See, for example, Peter Sandrev January 31, 2014 Deposition Transcript, pp. 26-27, 60-61; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 97-99; Jeremy Dooley December 2, 2013 Deposition Transcript, pp. 29-30.

[34] See Peter Sandrev January 31, 2014 Deposition Transcript, pp. 60-61.

[35] See, for example, Allen Truett February 27, 2014, Deposition Transcript, pp. 68-69, 78-79.

[36] See, for example, John Boyle February 5, 2013 Investigational Hearing Transcript, pp. 64-65; John Boyle January 28, 2014 Deposition Transcript, p. 12; July 12, 2011 Email from D. Rosenfeld to A. Sheer and R. Yodaiken (FTC-LABMD-003749 through FTC-LABMD-003750) (CX0449); FTC-LABMD-003624 through FTC-LABMD-003625 (CX0396) (APT "Contract Period" ran from August 2003 to March 2007).

Exhibit 3

B. Employee User Account Policy Claim

25. Mr. Fisk's Employee User Account Policy Claim is not supported by the record evidence. First, although Mr. Fisk contends that the policy restricting employee downloads was in place as of 2001, the version of the Employee User Account Policy that LabMD claims represents its security practices in 2007 and 2008 does not include the policy restricting employee downloads.[37]

26. In addition, the record shows that the Employee User Account Policy was not written until 2010. As I explained in my Initial Expert Report, it is important that security policies be in writing to provide guidance to employees who implement the policies and receive training about the policies, to facilitate changes to the policies as security threats evolve, and to communicate the policies to future employees.[38]

27. Second, contrary to Mr. Fisk's contention, there is no evidence in the record indicating that, as a manager, Ms. Woodson "likely needed access to unique applications to perform her job duties."[39] Nonetheless, the record evidence indicates that the policy restricting employee downloads, even if it had existed, was not enforced with respect to managers, like Ms. Woodson, before summer 2009.[40] In fact, former LabMD IT Manager, Robert Hyer, testified that, when he began working for LabMD as a contractor in summer 2009, one of the first things he did with respect to security was to implement technical measures to prevent all LabMD managers except

[37] Mr. Fisk cites to CX0007, see Fisk Report at 22-23, but LabMD claims that CX0006 represents its security practices in 2007 and 2008. See, for example, John Boyle February 5, 2013 Investigational Hearing Transcript, pp. 78-79, 98; August 30, 2010 Letter from P. Ellis to A. Sheer (FTC-LABMD-003132 through FTC-LABMD-003137) (CX0446). The version of the Employee User Account Policy in CX0007 includes the policy restricting employee downloads. See CX0007, page 21. The version in CX0006 does not. See CX0006, page 12.

[38] See Initial Expert Report, ¶ 53.

[39] Fisk Report, p. 23.

[40] See, for example, Robert Hyer December 13, 2013 Deposition Transcript, pp. 26-30, 33-35; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 171-172; Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 38-39.

Exhibit 3

the Vice President of Operations from downloading applications to their computers because "those constraints were not being administered as they should have been" prior to his arrival.[41]

C. Manual Inspections Claim

28. Mr. Fisk's Manual Inspections Claim is not true. Automated tools, such as File Integrity Monitors, are not only more efficient than manual inspections at discovering unauthorized applications and other risks and vulnerabilities on a network, they are also significantly more effective. As I explained in my Initial Report, even when conducted on a regular basis, manual computer inspections can never be exhaustive.[42] Human beings cannot inspect every place in a computer where vulnerabilities and risks can exist. Even if they could, malicious software may, in some instances, mask its presence to avoid detection during a manual inspection.[43] Furthermore, the record shows that, at least until mid-2008, LabMD manually inspected employee computers only when an employee complained about the computer's performance.[44]

29. Tellingly, LabMD's manual inspections never discovered that LimeWire was installed on the billing manager's computer even though it had been installed on the computer at least two years before Tiversa notified LabMD that it had found the 1,718 File on a P2P network. This illustrates the ineffectiveness of LabMD's manual inspection process.[45]

[41] See Robert Hyer December 13, 2013 Deposition Transcript, pp. 26-30, 33-35.

[42] See Initial Expert Report, ¶ 68(c).

[43] See Initial Expert Report, ¶ 68(c).

[44] See Initial Expert Report, ¶ 68(c).

[45] Mr. Fisk critiques my analysis concerning the risks associated with LabMD's use of SSL 2.0, noting that IIS 7.0 shipped with SSL 2.0 enabled by default. See Fisk Report at 31. Mr. Fisk does not, however, dispute that Microsoft warned about the vulnerabilities in SSL 2.0 as early as 2007. LabMD could have easily addressed those vulnerabilities by following instructions provided by Microsoft, which would disable SSL 2.0 and enable a more secure version of SSL, version 3.0/TLS 1.0. Mr. Fisk's observation that yahoo.com supports SSL 2.0 is not relevant because it fails to take into account the large amounts of highly sensitive Personal Information that LabMD maintained on its network during the Relevant Time Period.

Exhibit 3

V. Conclusion

30. Based on my evaluation of the Fisk Report, my review of the materials described in Paragraph 3, above, and my experience described in Section II of my Initial Expert Report, I conclude that Mr. Fisk's opinion that "LabMD's security was reasonable and adequate" to protect the Personal Information maintained on its network is unreliable and fundamentally flawed because his analysis of the adequacy of LabMD's security practices:

a. Fails to address the goals, policies, and mechanisms of a comprehensive information security program implementing a defense in depth strategy; and

b. Is not supported by the record evidence.

31. Nothing in the Fisk Report changes my conclusion that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, or the opinions that I provided in my Initial Expert Report in support of that conclusion.

Dated: April 11, 2014

Raquel Hill

Raquel Hill, Ph.D.

Exhibit 3

Appendix A

Exhibit 3

Appendix A

Web Content Considered or Relied Upon

- BitTorrent For Developers, http://www.bittorrent.org/beps/bep_0003.html, last accessed April 11, 2014.
- Cisco 1841 Integrated Services Router, http://www.cisco.com/c/en/us/products/routers/1841-integrated-services-router-isr/index.html, last accessed April 11, 2014.
- Federal Communications Commission Small Biz Cyber Planner 2.0, http://www.fcc.gov/cyberplanner, last accessed April 11, 2014.
- Gnutella Protocol Development, http://rfc-gnutella.sourceforge.net/developer/index.html, last accessed April 11, 2014.
- LittleShoot P2P File Sharing Browser, http://www.littleshoot.org/, last accessed April 11, 2014.
- Microsoft Support – How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services, http://support.microsoft.com/kb/187498, last accessed April 11, 2014.
- MSDN Blogs – Support for SSL/TLS protocols on Windows, http://blogs.msdn.com/b/kaushal/archive/2011/10/02/support-for-ssl-tls-protocols-on-windows.aspx, last accessed April 11, 2014.
- Symantec – VERITAS Backup Exec for Windows Servers, http://securityresponse.symantec.com/avcenter/security/Content/2005.08.12b.html, last accessed April 11, 2014.
- ZyWall Firewall, http://help.zyxel.com/documents/webhelp/zwp1/401XJ0/en/h_Fire_DefaultRule-Router.html, last accessed April 11, 2014.

Articles & Publications Considered or Relied Upon

- Bloomberg BusinessWeek, "The Scent of Easy Prey" (March 14, 2001), http://www.businessweek.com/stories/2001-03-14/the-scent-of-an-easy-prey, last accessed April 11, 2014.
- Federal Communications Commission, "Cyber Security Planning Guide", http://transition.fcc.gov/cyber/cyberplanner.pdf, last accessed April 11, 2014.
- Muncaster, Phil, The Register, "Dimmed but not out: Lantern anti-censorship tool blocked in China" (December 12, 2013), http://www.theregister.co.uk/2013/12/12/lantern_censorship_blocked_great_firewall/, last accessed April 11, 2014.
- National Security Agency, "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments", http://www.nsa.gov/ia/_files/support/defenseindepth.pdf, last accessed April 11, 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 April 11, 2014.

Exhibit 3

- SANS Institute InfoSec Reading Room, “Peer-to-Peer File-Sharing Networks: Security Risks” (2002), https://www.sans.org/reading-room/whitepapers/policyissues/peer-to-peer-file-sharing-networks-security-risks-510, last accessed April 11, 2014.
- VERITAS Datasheet, “VERITAS Backup Exec 10 for Windows Servers” (2004), http://eval.veritas.com/mktginfo/products/Datasheets/Data_Protection/bews_10_options_datasheet.pdf, last accessed April 11, 2014.

Exhibit 3

EXHIBIT 4

In the Matter of:

LabMD, Inc.

February 5, 2013
John Boyle

Condensed Transcript with Word Index

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

Exhibit 4

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 5

In the Matter of:

LabMD, Inc.

March 4, 2014
Michael Daugherty

Condensed Transcript with Word Index

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

Exhibit 5

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 6

In the Matter of:

LabMD, Inc.

May 3, 2013
Curt Kaloustian

Condensed Transcript with Word Index

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

Exhibit 6

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 7

Last	First	Position
Gilmore	Nena	Accessioning Mgr
Bellvue	Rose	Billing
Woodson	Rosalind	Billing Mgr
Brown	Sandra	Billing Rep
Garrett	Karalyn	Billing Rep
Harris	Nicotra	Billing Rep
Roberson-Wright	Bianca	Billing Rep
Starks	Jamie	Billing Rep
Washington	Jani	Billing Rep
Fair	Liz	Billing/Client Services Mgr
Diakow	Cindy	Exec Asst
Gilbreth	Tricia	Finance Mgr
Bradley	Brandon	IT
Bureau	Matt	IT
Elliott	Nicole	IT
Howard	Pat	IT
Kaloustian	Curt	IT
Maire	Christopher	IT
Parr	Jennifer	IT
Simmons	Alison	IT
Hyer	Bob	IT Mgr
Martin	Jeff	IT Mgr
Bagwell	Dean'na	Lab Asst
Miller	Chad	Lab Mgr
Warvin	Connie	Lab Mgr
Ghashghaei	Mandana	Med Tech
Haynes	Lindsey	Med Tech
Patel	Palak	Med Tech
Paull	Gerson	Pathologist
Pennington	Marian	Pathologist
Stevenson	Alan	Pathologist
Savera	Adnan	Phlebotomist
Daugherty	Michael	President
Jordan	Sherry	Transcriptionist

Exhibit 7

Boyle	John	Vice Pres/GM

Exhibit 7

Information Access
Medical and Billing
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Billing and *Limited Medical
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing
Medical and Billing

Exhibit 7

Medical and Billing

*People employed in the billing department had limited access to medical information which allowed them to properly code the bill for services

*Pursuant to the definition of "Personal Information" in the definition section of Complaint Counsel's First Set of Interrogatories, all of the people of above listed had various levels of access to: (a) first and last name; (b) telephone number; (c) a home or other physical address; (d) date of birth; (e) Social Security Number; (f) medical record number; (g) bank routing, account, and checknumbers; (h) credit or deibt card information; (i) laboratory test result, medical test code, diagnosis or clincal history; or (j) health insurance company name and policy

Exhibit 7

Exhibit 7

provided.

Exhibit 7

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

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

RESPONDENT'S SUPPLEMENTAL RESPONSE TO COMPLAINT COUNSEL'S FIRST SET OF INTERROGATORIES

Respondent, LabMD, Inc. ("LabMD"), supplements its response to Complaint Counsel's First Set of Interrogatories as follows:

2. For each Person identified in response to Interrogatory No. 1, state the types of Personal Information that the Person had authority to access.

Answer: Respondent objects to this Interrogatory to the extent that it is vague and ambiguous and seeks information which is neither relevant nor reasonably calculated to lead to the discovery of admissible evidence. Specifically, Complaint Counsel's use of the phrase "authority to access" is ambiguous. Without waiving these objections and/or the foregoing General Objections, Respondent states that it is unable to answer this Interrogatory as worded, but states 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. Moreover, Respondent points out that despite numerous depositions of LabMD employees by Complaint Counsel, including IT personnel, no deponent has been able to state precisely the type of Personal Information each employee had access to during their entire period employment from January 2005 through the present. According to the deposition testimony, most LabMD employees were aware that they had access to sufficient information to perform their jobs but

Exhibit 7

that they did not have access to all information on the system. Respondent further states neither Mike Daugherty nor Jeff Martin were able to provide the precise information that would be responsive to this Interrogatory as worded.

/s/ William A. Sherman, II__
Reed D. Rubinstein, Esq.
William A. Sherman, II, Esq.
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW Suite 610
Washington, DC 20004
Phone: (202) 372-9100
Facsimile: (202) 372-9141
Email: william.sherman@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 administrative proceedings before federal agencies.
Counsel for Respondent

Exhibit 7

CERTIFICATE OF SERVICE

This is to certify that on March 17, 2014, I served via electronic mail delivery a copy of the foregoing document to:

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
Complaint Counsel
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW Room NJ-8100
Washington, DC 20580
Tel: (202) 326-2999 (VanDruff) Facsimile: (202) 326-3062
Email: lvandruff@ftc.gov

By: /s/ William A. Sherman, II

552284v1

Exhibit 7

EXHIBIT 8

In the Matter of:

LabMD, Inc.

January 11, 2014
Sandra Brown

Condensed Transcript with Word Index

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

Exhibit 8

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 9

In the Matter of:

LabMD, Inc.

January 10, 2014
Matthew Stuart Bureau

Condensed Transcript with Word Index

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

Exhibit 9

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 10

In the Matter of:

LabMD, Inc.

February 7, 2014
Patricia Gilbreth

Condensed Transcript with Word Index

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

Exhibit 10

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 11

In the Matter of:

LabMD, Inc.

December 13, 2013
Robert W. Hyer

Condensed Transcript with Word Index

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

Exhibit 11

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 12

In the Matter of:

LabMD, Inc.

February 14, 2014
Brandon Bradley

Condensed Transcript with Word Index

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

Exhibit 12

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 13

Analysis Date	Friday - May 21, 2010
Type of Analysis	Full Report
Overall Security Posture	Poor (100%)
Threats Discovered	32 (Risk: 5=1, 4=1, 3=2, 2=3, 1=25)
Total Hosts Scanned	1 (1 severe)
Scan Date(s)	- Wednesday - May 19, 2010
Scanners Used	- EXTERNAL (140.99.20.86, 140.99.20.85)
Scan Options Used	- Port Scan: 1,000 most common using syn packets - Safe Tests Only - Paranoid Threat Reporting - Scan Speed: Medium - Scan Dead Hosts

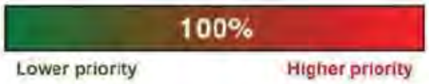
Exhibit 13

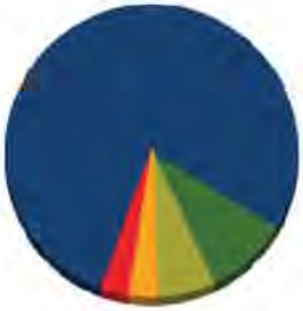
Executive Summary

This document provides the results of the vulnerability assessment performed by Security for Your Company. The information contained within this document is considered extremely confidential and should be treated as such.

The graph below represents the seriousness of the security threats found during the assessment. The higher the percentage, the higher the priority should be for resolving the discovered security threats.

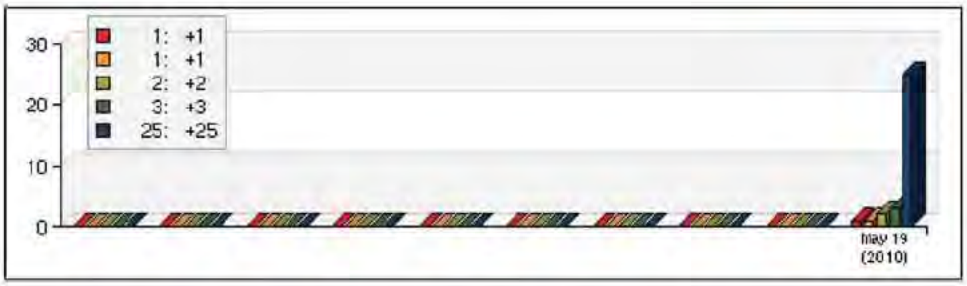
Risk 5	1	3.12%
Risk 4	1	3.12%
Risk 3	2	6.25%
Risk 2	3	9.38%
Risk 1	25	78.12%





The scope of this analysis was to remotely audit and analyze the system and/or resources of each host in this assessment. This provides a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack.

The graph below gives a historical perspective of the number of known security threats discovered for these hosts. Drastic changes indicate that something has impacted the security posture of these hosts and should be looked into immediately.



The chart below shows how the potential security threats are spread across different families of threat classifications. A large diversification of families (> 4) is cause for concern because these types of systems make for a more desirable target for potential attackers. A relatively minor threat in one service could help an attacker exploit a more difficult and significant threat in another service.

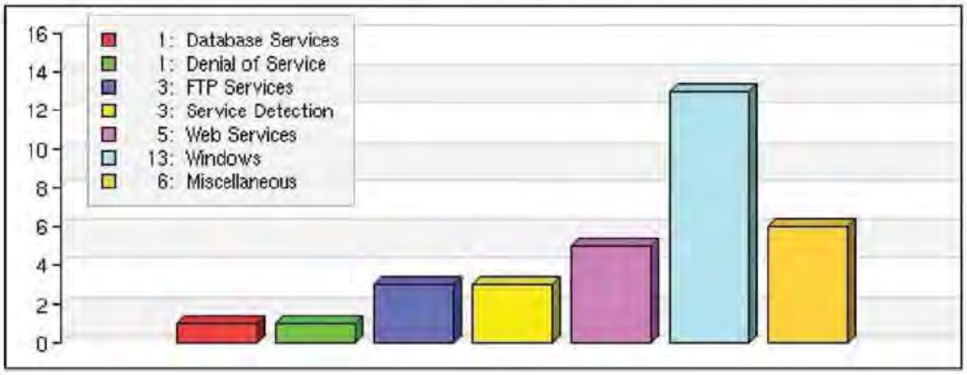


Exhibit 13

Scope of Assessment

All of the hosts part of this assessment are listed in this section. 0 hosts were not scanned because they were inactive and the Ignore Dead Hosts option was set. 8 hosts were scanned but not selected for inclusion in this report. 1 hosts are listed in the table below along with some information to help determine if there were any issues during the scan that may have affected the results.

Of note are the Scan Time, Packet Loss, and Flags. The flags are described in the legend below. A non-zero packet loss is a sign that there was some kind of congestion between the scanner and that host. 100% packet loss usually means the host was not active, heavily firewalled to not allow any incoming traffic, or blacklisted by an Intrusion Prevention System (IPS). The scans are configured to not be stealthy intentionally. Scan times can vary considerably. The primary factor affecting how long a scan takes is the network between the scanner and target, specifically latency and packet filtering. The scan times are shown in hours and minutes (HH:MM). A legend for the various flags used is provided below:

Flag	Description
L	**Is Latest:** This flag indicates that the scan results being viewed for the host are the most recent.
D	**Is Dead or Blacklisted:** This flag is set when it looks like the host was already dead or died during the scan. For hosts returning no open ports or vulnerabilities, a stealthy probe will be performed to determine if the scanner appeared to have been blacklisted.
T	**Timed Out:** Abnormally long-running scans will be aborted automatically. 24 hours is allowed the port scan phase and 24 hours for the vulnerability assessment phase. If either phase takes longer than these hard limits, we will kill the process and flag the scan as timed out. It is possible that some results will be returned for a timed out scan. However, the completeness of the results cannot be determined.
P	**Unusual Number of Open Ports:** Some targets will show an obnoxious amount of ports as open, probably intentionally as a protection against port scanning. When 200 or more ports are returned as open, all port scan results will be automatically removed.
B	**Is Current Baseline:** Any previous scan can be defined as the baseline to use in the differential analysis. If a baseline has not been explicitly set, then the next latest scan will be used automatically.

SCANNER: EXTERNAL

Host and Operating System	Risk	Scan Time	Packet Loss	Flags
64.190.124.7 (64-190-124-7.static.cypresscom.net)	5	00:29	0%	L D

The following hosts from this assessment were scanned but not included in this report:

64.190.124.1-64.190.124.3, 64.190.124.5, 64.190.124.8-64.190.124.10, 64.190.124.14

Exhibit 13

Vulnerable Hosts

This Security Scan analysis scanned 1 total IP addresses. Of those, 1 host was found active with outstanding vulnerabilities or open ports. The following table provides a brief summary about each of these active hosts and their analysis data.

SCANNER: EXTERNAL

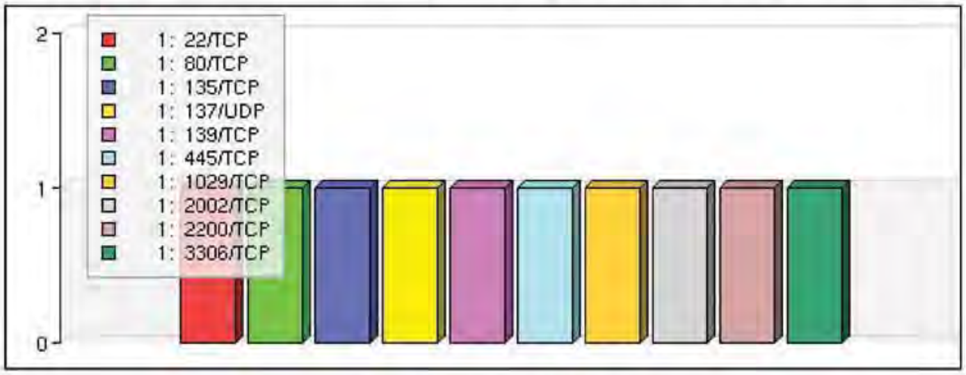
Host	Ports	5	4	3	2	1	Threats
64.190.124.7	14	1	1	2	3	25	32
Totals:	14	1	1	2	3	25	32

Exhibit 13

Discovered Open Ports (Nmap)

This assessment discovered a total of 14 distinct open network ports on the hosts in this report. This does not mean each open port is a security threat, but it does show some possible points of entry to your network that an attacker could potentially leverage. It is generally considered good practice to keep the number of open ports to a minimum. Sometimes hackers will target computers with a large number of open network ports because they may be more susceptible to attack. Minimizing the number of open network ports will help to minimize this risk and make your network less "attractive" to hackers and attacks.

A cross-reference of all discovered security threats by port number and risk factor is provided below. This analysis will help to determine which port represents the greatest overall risk to the target system. The most vulnerable port has been highlighted.



Number of Hosts vs. Open Ports

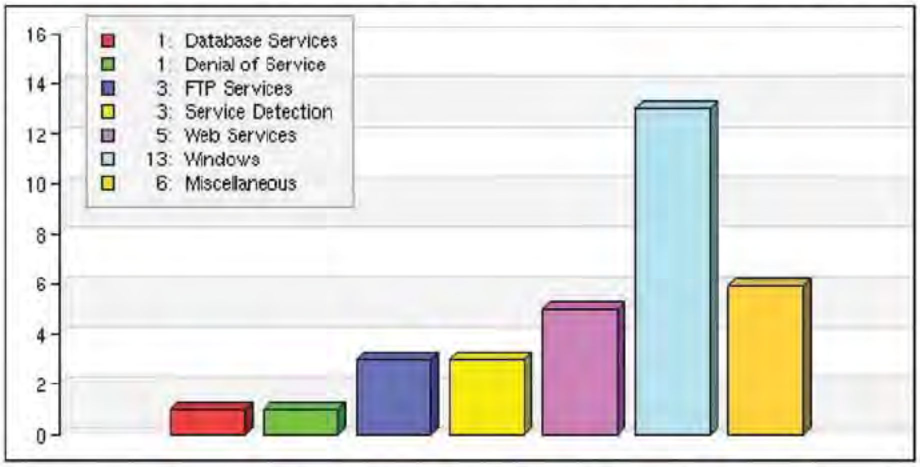
HOST: 64.190.124.7

Port	Service Type (estimated)	5	4	3	2	1	Total
ICMP		0	0	0	0	0	0
TCP		0	0	1	1	3	5
TCP:21	MICROSOFT FTPD	1	0	0	2	1	4
TCP:22	VANDYKE VSHELL SSHD 2.2.6.601 (PROTOCOL 2.0)	0	0	0	0	2	2
TCP:80	MICROSOFT IIS WEBSERVER 6.0	0	0	0	0	5	5
TCP:135	MICROSOFT WINDOWS RPC	0	0	0	0	1	1
TCP:137	---	0	0	0	0	1	1
UDP:137	NETBIOS-NS	0	0	0	0	0	0
TCP:139	NETBIOS-SSN	0	0	0	0	1	1
TCP:445	MICROSOFT WINDOWS 2003 MICROSOFT-DS	0	1	0	0	7	8
TCP:1025	MICROSOFT WINDOWS RPC	0	0	0	0	1	1
TCP:1029	MICROSOFT WINDOWS RPC	0	0	0	0	1	1
TCP:2002	SSL/GLOBE?	0	0	0	0	1	1
TCP:2200	UNKNOWN	0	0	0	0	0	0
TCP:3306	MYSQL 5.1.22-RC-COMMUNITY	0	0	1	0	1	2

Exhibit 13

Vulnerable Threat Families

The 32 total discovered vulnerabilities are spread across 7 families of threat classifications. The graph below shows the most frequently occuring threat families discovered on this network. Also, a complete list of every threat classification along with the number of vulnerabilities discovered is in the table below. The most vulnerable family has been highlighted.



Number of Discovered Threats vs. Family Classifications

Family	5	4	3	2	1	Total
Database Services	0	0	1	0	0	1
Denial of Service	0	0	0	1	0	1
FTP Services	1	0	0	2	0	3
Miscellaneous	0	0	1	0	5	6
Service Detection	0	0	0	0	3	3
Web Services	0	0	0	0	5	5
Windows	0	1	0	0	12	13

Exhibit 13

Discovered Security Threats Summary

This section provides a simple one-line summary of each discovered potential security threat on each host in this network. These summaries are grouped by host and sorted by risk factor. The full analysis report for each host is linked to the IP address.

HOST: 64.190.124.7

Risk	Port	ID	Summary
5	TCP:21	110088	Anonymous FTP Writeable root Directory
4	TCP:445	118028	MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066) (uncredentialed check)
3	TCP	110919	Open Port Re-check
3	TCP:3306	129345	MySQL Community Server < 5.1.23 / 6.0.4 Multiple Vulnerabilities
2	TCP	112213	TCP/IP Sequence Prediction Blind Reset Spoofing DoS
2	TCP:21	110079	Anonymous FTP Enabled
2	TCP:21	134324	FTP Supports Clear Text Authentication
1	TCP	110114	ICMP Timestamp Request Remote Date Disclosure
1	TCP	111936	OS Identification
1	TCP	135716	Ethernet card brand
1	TCP:21	110092	FTP Server Detection
1	TCP:22	110267	SSH Server Type and Version Information
1	TCP:22	110881	SSH Protocol Versions Supported
1	TCP:80	110107	HTTP Server Type and Version
1	TCP:80	124260	HyperText Transfer Protocol (HTTP) Information
1	TCP:80	143111	HTTP methods per directory
1	TCP:80	400000	Potentially sensitive resource discovered
1	TCP:80	403092	Interesting Web Document Found
1	TCP:135	110736	DCE Services Enumeration
1	TCP:137	110150	Using NetBIOS or SMB to retrieve information from a Windows host
1	TCP:139	111011	SMB Service Detection
1	TCP:445	110394	SMB Log In Possible
1	TCP:445	110397	SMB LanMan Pipe Server Listing Disclosure
1	TCP:445	110736	DCE Services Enumeration
1	TCP:445	110785	SMB NativeLanManager Remote System Information Disclosure
1	TCP:445	111011	SMB Service Detection
1	TCP:445	126917	SMB registry can not be accessed by the scanner
1	TCP:445	126920	SMB NULL Session Authentication
1	TCP:1025	110736	DCE Services Enumeration
1	TCP:1029	110736	DCE Services Enumeration

Exhibit 13

1	TCP:2002	121643	SSL Cipher Suites Supported
1	TCP:3306	111153	Unknown Service Detection: HELP Request

Exhibit 13

Threat Differential

This section lists all of the differences in discovered threats for all hosts in this assessment. Differences are derived based on the results obtained during the baseline scan.

This table shows the relative risks that exist on the hosts in this assessment and the remediation trends of said risks for the period of 2010-05-19 - 2010-05-19.

	5	4	3	2	1
Threats resolved since the baseline scan:	0	0	0	0	0
Threats discovered since the baseline scan:	0	0	0	0	0
Current outstanding threats:	1	1	2	3	25

There are no differences to report among all active hosts.

These hosts from this assessment are considered new since only scanned once:
64.190.124.7

Exhibit 13

Network Characteristics

This section is not specific to security threats or vulnerabilities. Rather, the Network Characteristics section provides general information about how each host in this assessment responded to some standard basic network testing. The information in this section may be useful to gain an understanding of the characteristics of the hosts as seen from a remote network across the Internet.

Exhibit 13

Response Times and Packet Loss

Although ping is sometimes considered a valuable network diagnostic tool, it can also sometimes be used for certain denial of service (DoS) attacks. You should consider the possible impact this may, or may not, have on your network resources.

The table below lists the packet loss and round-trip times (ms) for each host in this assessment. Non-zero packet loss is a sign of too much network traffic. A significant amount of packet loss may skew the results of the entire assessment. Please note, however, that hosts that have no open ports and are rejecting ICMP Echo requests will report 100% packet loss.

Host	Packet Loss	Min	Avg	Max
64.190.124.7	0%	48.7	49.3	51.4

Exhibit 13

Reverse DNS Information

Reverse DNS records are necessary for some network protocols and/or applications to function correctly. It is always a good idea to give an IP address a valid reverse DNS record, even if it is just a generic name within your domain. The results from attempting to resolve each host in this assessment are shown below.

IP Address	Reverse DNS	Resolved By	Authoritative Server
64.190.124.7	64-190-124-7.static.cypresscom	140.99.20.76	loyal.cypresscomm.com.

Exhibit 13

Traceroute Response

The information below shows the round-trip times for each responsive hop between the scanner and target host in this assessment. This traceroute was performed using a maximum TTL value of 30, one UDP query per TTL, and a starting TTL of 5.

HOST: 64.190.124.7

Hop	IP Address	Hostname	Time (ms)
5	4.69.133.30	ae-8-8.ebr1.Dallas1.Level3.net	36.38
6	4.69.146.76	ae-73-78.ebr3.Dallas1.Level3.net	25.13
8	4.68.103.37	ge-11-0.hsa2.Atlanta1.Level3.net	44.72
9	4.79.226.46	CYPRESS.hsa2.Atlanta1.Level3.net	45.01
10	10.1.2.18		45.22
11	64.190.74.129	64-190-74-129.static.cypresscom.net	50.14
12	64.190.124.7	64-190-124-7.static.cypresscom.net	49.21

Exhibit 13

SMB Shares

The following SMB shares were discovered.

HOST: 64.190.124.7

Share	Type	Comment
WORKGROUP	Workgroup	MAPPER
LABMD	Workgroup	VISNETIC

Exhibit 13

Online Public Database Search

There are various public databases, accessible via the Internet, which may contain information about your network, systems, and company. Under normal circumstances, this information is not confidential and does not contain any errors. However, it is also possible for these public databases to contain sensitive and/or incorrect data. If this is the case, the potential impact could vary widely. It may be a simple typo, it may allow your network to be hijacked by hackers, or it may expose proprietary information to the Internet.

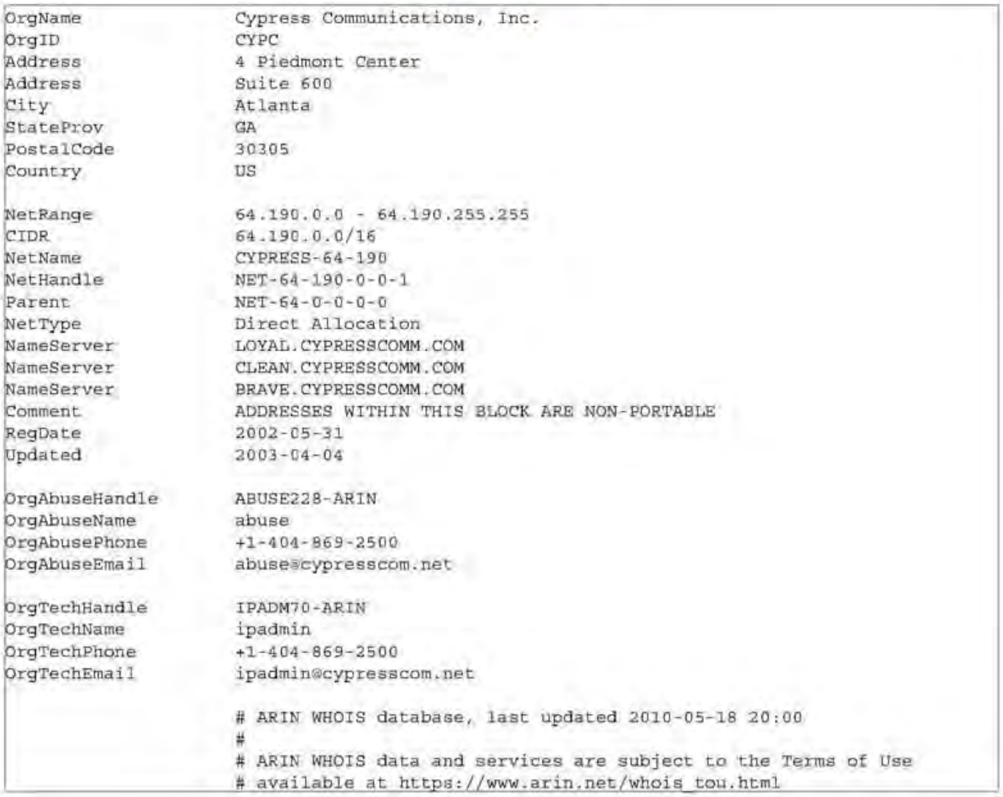
In the sections Whois Domain and Whois Arin, online public databases were queried for information about each host in this assessment. Because this information is specific to your network, Security can not automatically determine if this information is correct or not. Please review the results listed in those sections for each of these queries to ensure that the information is both correct and non-confidential.

Exhibit 13

IP Address Registries

The ARIN IP Address registry was queried for each host in this assessment. The results of this query should show the owner (and associated contacts) for each host. This should probably be your company directly, your ISP, or maybe even your hosting provider (if applicable). The entity listed below is considered the authoritative owner of the host.

HOST(s): 64.190.124.7



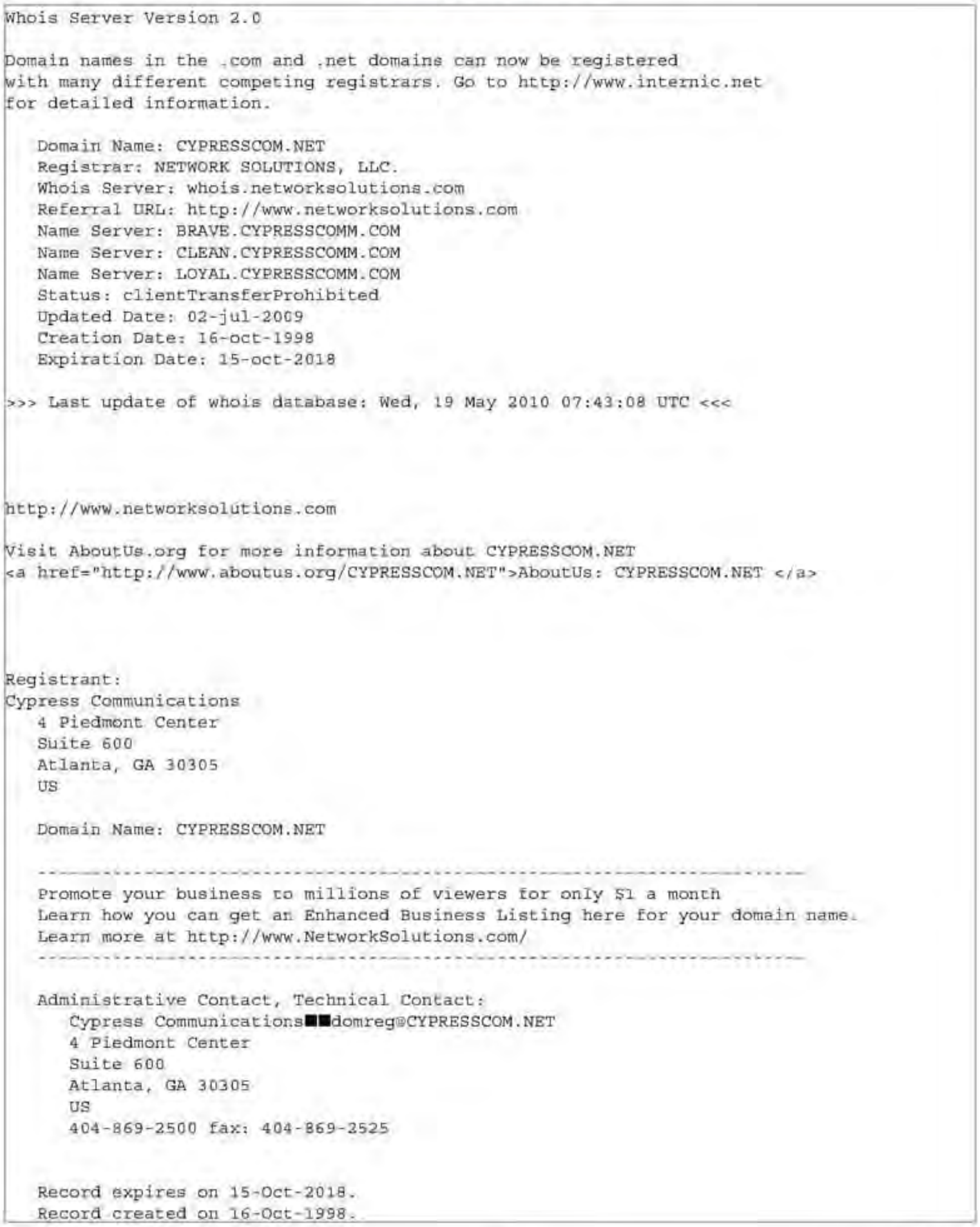
```
OrgName             Cypress Communications, Inc.
OrgID               CYPC
Address             4 Piedmont Center
Address             Suite 600
City                Atlanta
StateProv           GA
PostalCode          30305
Country             US

NetRange            64.190.0.0 - 64.190.255.255
CIDR                64.190.0.0/16
NetName             CYPRESS-64-190
NetHandle           NET-64-190-0-0-1
Parent              NET-64-0-0-0-0
NetType             Direct Allocation
NameServer          LOYAL.CYPRESSCOMM.COM
NameServer          CLEAN.CYPRESSCOMM.COM
NameServer          BRAVE.CYPRESSCOMM.COM
Comment             ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate             2002-05-31
Updated             2003-04-04

OrgAbuseHandle      ABUSE228-ARIN
OrgAbuseName        abuse
OrgAbusePhone       +1-404-869-2500
OrgAbuseEmail       abuse@cypresscom.net

OrgTechHandle       IPADM70-ARIN
OrgTechName         ipadmin
OrgTechPhone        +1-404-869-2500
OrgTechEmail        ipadmin@cypresscom.net

                    # ARIN WHOIS database, last updated 2010-05-18 20:00
                    #
                    # ARIN WHOIS data and services are subject to the Terms of Use
                    # available at https://www.arin.net/whois_tou.html
```

Exhibit 13

Domain Name Registries

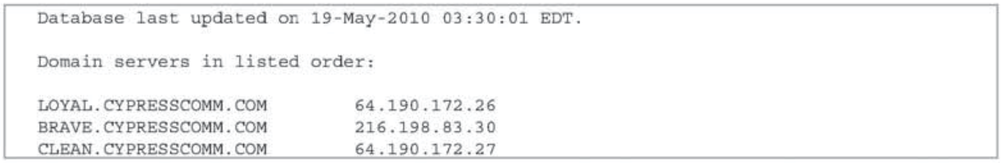
This section attempted to resolve the domain name for each host in this assessment. Then, that domain name, if any, was searched in the Internic and domain name registry databases. The results of this query should report the owner (and associated contacts) for the domain name, if any, associated the host. This should probably be your company directly, your ISP, or maybe even your hosting provider (if applicable). The entity listed below is considered the authoritative owner of the domain name, if any, associated with the host.

HOST(s): 64.190.124.7



```
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: CYPRESSCOM.NET
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com
   Name Server: BRAVE.CYPRESSCOMM.COM
   Name Server: CLEAN.CYPRESSCOMM.COM
   Name Server: LOYAL.CYPRESSCOMM.COM
   Status: clientTransferProhibited
   Updated Date: 02-jul-2009
   Creation Date: 16-oct-1998
   Expiration Date: 15-oct-2018

>>> Last update of whois database: Wed, 19 May 2010 07:43:08 UTC <<<



http://www.networksolutions.com

Visit AboutUs.org for more information about CYPRESSCOM.NET
<a href="http://www.aboutus.org/CYPRESSCOM.NET">AboutUs: CYPRESSCOM.NET </a>



Registrant:
Cypress Communications
   4 Piedmont Center
   Suite 600
   Atlanta, GA 30305
   US

   Domain Name: CYPRESSCOM.NET

   -------------------------------------------------------------------------
   Promote your business to millions of viewers for only $1 a month
   Learn how you can get an Enhanced Business Listing here for your domain name.
   Learn more at http://www.NetworkSolutions.com/
   -------------------------------------------------------------------------

   Administrative Contact, Technical Contact:
      Cypress Communications■■domreg@CYPRESSCOM.NET
      4 Piedmont Center
      Suite 600
      Atlanta, GA 30305
      US
      404-869-2500 fax: 404-869-2525


   Record expires on 15-Oct-2018.
   Record created on 16-Oct-1998.
```

Exhibit 13



```
Database last updated on 19-May-2010 03:30:01 EDT.

Domain servers in listed order:

LOYAL.CYPRESSCOMM.COM        64.190.172.26
BRAVE.CYPRESSCOMM.COM        216.198.83.30
CLEAN.CYPRESSCOMM.COM        64.190.172.27
```

Exhibit 13

Discovered Security Threats by Host

This section provides all the details about each discovered potential security threat for all of the hosts in this assessment. These details are grouped by host and ordered by risk factor.

HOST: 64.190.124.7

	ID	Port	Risk
Anonymous FTP Writeable root Directory			
FTP Services :: Nessus	110088	TCP:21	5

It is possible to write on the root directory of this remote anonymous FTP server. This allows an attacker to upload arbitrary files which could be used in other attacks, or to turn the FTP server into a software distribution point.

Solution:

Restrict write access to the root directory.

CVSS Information:

Low Attack Complexity, Complete Confidentiality Impact, Complete Integrity Impact, Complete Availability Impact

Additional References:

CVE-1999-0527, OSVDB-76, http://www.cert.org/advisories/CA-1993-10.html

	ID	Port	Risk
MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066) (uncredentialed check)			
Windows :: Nessus	118028	TCP:445	4

The remote host runs a version of Windows that has a flaw in its TCP/IP stack.

The flaw may allow an attacker to execute arbitrary code with SYSTEM privileges on the remote host or to perform a denial of service attack against the remote host.

Proof of concept code is available to perform a denial of service attack against a vulnerable system.

http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx

Solution:

Microsoft has released a set of patches for Windows 2000, XP and 2003 :

CVSS Information:

Low Attack Complexity, Partial Confidentiality Impact, Partial Integrity Impact, Complete Availability Impact

Additional References:

CVE-2005-0048, CVE-2004-0790, CVE-2004-1060, CVE-2004-0230, CVE-2005-0688, Bugtraq-13124, Bugtraq-13116, OSVDB-4030, OSVDB-14578, OSVDB-15457, OSVDB-15463, OSVDB-15619, http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx

	ID	Port	Risk
Open Port Re-check			
Miscellaneous :: Nessus	110919	TCP	3

One of several ports that were previously open are now closed or unresponsive. There are numerous possible causes for this failure:

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process

This might be an availability problem related to the following reasons:

- A network outage has been experienced during the scan, and the remote network cannot be reached from the Vulnerability Scanner any more.

Exhibit 13

- This Vulnerability Scanner has been blacklisted by the system administrator or by automatic intrusion detection/prevention systems which have detected the vulnerability assessment.

- The remote host is now down, either because a user turned it off during the scan or because a select denial fo service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again. The traceroute information may provide insight as to which device is interfering with the scan.

Solution:

1. Use a slower scan speed setting.
2. Disable your IPS during the scan.
3. Review packet filters on target.

Information from Target:

Connections to this host from the scanner with IP address 140.99.20.86 were blocked on 2010-05-19 08:13:08 (GMT). The following ports are no longer responsive: 2002.

MySQL Community Server < 5.1.23 / 6.0.4 Multiple Vulnerabilities	ID	Port	Risk
Database Services :: Nessus	129345	TCP:3306	3

The version of MySQL Server installed on the remote host reportedly is affected by the following issues :

- It is possible, by creating a partitioned table using the DATA DIRECTORY and INDEX DIRECTORY options, to gain privileges on other tables having the same name as the partitioned table. (Bug #32091)

- Using RENAME TABLE against a table with explicit DATA DIRECTORY and INDEX DIRECTORY options can be used to overwrite system table information. (Bug #32111).

- ALTER VIEW retains the original DEFINER value, even when altered by another user, which can allow that user to gain the access rights of the view. (Bug #29908)

- When using a FEDERATED table, the local server can be forced to crash if the remote server returns a result with fewer columns than expected. (Bug #29801)

Solution:

Upgrade to MySQL Community Server version 5.1.23 / 6.0.4 or later.

CVSS Information:

Partial Confidentiality Impact, Partial Integrity Impact, Partial Availability Impact

Additional References:

CVE-2007-5969, CVE-2007-5970, CVE-2007-6303, CVE-2007-6304, Bugtraq-26765, Bugtraq-26832, OSVDB-42607, OSVDB-42608, OSVDB-42609, OSVDB-42610, http://bugs.mysql.com/32091, http://bugs.mysql.com/32111, http://bugs.mysql.com/29908, http://bugs.mysql.com/29801, http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html, http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html

Information from Target:

The remote MySQL Community Server's version is :

5.1.22-rc-community

TCP/IP Sequence Prediction Blind Reset Spoofing DoS	ID	Port	Risk
Denial of Service :: Nessus	112213	TCP	2

Exhibit 13

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution:

See http://www.securityfocus.com/bid/10183/solution/

CVSS Information:

Low Attack Complexity, Partial Availability Impact

Additional References:

CVE-2004-0230, Bugtraq-10183, OSVDB-4030, IAVA-2004-A-0007, http://www.securityfocus.com/bid/10183/solution/

Anonymous FTP Enabled	ID	Port	Risk
FTP Services :: Nessus	110079	TCP:21	2

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Solution:

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

CVSS Information:

Low Attack Complexity, Partial Confidentiality Impact

Additional References:

CVE-1999-0497, OSVDB-69

FTP Supports Clear Text Authentication	ID	Port	Risk
FTP Services :: Nessus	134324	TCP:21	2

The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.

Solution:

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.

CVSS Information:

Partial Confidentiality Impact

ICMP Timestamp Request Remote Date Disclosure	ID	Port	Risk
Miscellaneous :: Nessus	110114	TCP	1

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Solution:

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Additional References:

CVE-1999-0524, OSVDB-94

Exhibit 13

Information from Target:
The ICMP timestamps seem to be in little endian format (not in network format)

The difference between the local and remote clocks is 655 seconds.

OS Identification	ID	Port	Risk
Miscellaneous :: Nessus	111936	TCP	1

This script attempts to identify the Operating System type and version by looking at the results of other scripts

Information from Target:
Remote operating system : Microsoft Windows Server 2003 Service Pack 2
Confidence Level : 99
Method : MSRPC

The remote host is running Microsoft Windows Server 2003 Service Pack 2

Ethernet card brand	ID	Port	Risk
Miscellaneous :: Nessus	135716	TCP	1

Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'. These OUI are registered by IEEE.

Additional References:

http://standards.ieee.org/faqs/OUI.html, http://standards.ieee.org/regauth/oui/index.shtml

Information from Target:
The following card manufacturers were identified :

00:19:b9:d1:58:e9 : Dell Inc.

FTP Server Detection	ID	Port	Risk
Service Detection :: Nessus	110092	TCP:21	1

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

Information from Target:
The remote FTP banner is :

220 Microsoft FTP Service

SSH Server Type and Version Information	ID	Port	Risk
Service Detection :: Nessus	110267	TCP:22	1

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Information from Target:
SSH version : SSH-2.0-VShell_2_2_6_601 VShell

SSH supported authentication : publickey,password

SSH Protocol Versions Supported	ID	Port	Risk
Miscellaneous :: Nessus	110881	TCP:22	1

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Exhibit 13

Information from Target:
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : 7e:27:5b:6e:ab:f4:c3:8c:4f:a1:4e:be:b7:77:2c:b2

HTTP Server Type and Version	ID	Port	Risk
Web Services :: Nessus	110107	TCP:80	1

This plugin attempts to determine the type and the version of the remote web server.

Information from Target:
The remote web server type is :

Microsoft-IIS/6.0

HyperText Transfer Protocol (HTTP) Information	ID	Port	Risk
Web Services :: Nessus	124260	TCP:80	1

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc. This test is informational only and does not denote any security problem.

Information from Target:
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Length: 1539
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 19 May 2010 07:56:17 GMT

HTTP methods per directory	ID	Port	Risk
Web Services :: Nessus	143111	TCP:80	1

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Exhibit 13

Information from Target:
Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/

Potentially sensitive resource discovered	ID	Port	Risk
Web Services :: Nikto	400000	TCP:80	1

Path: /

The Nikto web application scanner found an interesting file/url. It is recommended to verify that this resource does not contain any sensitive information and is intended to be available to the public. If this is a legitimate resource, then this file/url can be marked to be ignored from future reporting.

Information from Target:

Microsoft-IIS/6.0 appears to be outdated (4.0 for NT 4, 5.0 for Win2k, current is at least 7.0)

Interesting Web Document Found	ID	Port	Risk
Web Services :: Nikto	403092	TCP:80	1

Path: /localstart.asp

A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.

Solution:

If the file or directory contains sensitive information, remove the files from the web server or password protect them.

Additional References:

OSVDB-3092

DCE Services Enumeration	ID	Port	Risk
Windows :: Nessus	110736	TCP:135	1

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Exhibit 13

Information from Target:

The following DCERPC services are available locally :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : DNSResolver

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : trkwks

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : SECLOGON

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : keysvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : W32TIME_ALT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Unknown RPC service
Annotation : Unimodem LRPC Endpoint
Type : Local RPC service
Named pipe : tapsrvlpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Unknown RPC service
```

Exhibit 13

```
Annotation : Unimodem LRPC Endpoint
Type : Local RPC service
Named pipe : unimdmsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0
Internet Information Service (IISAdmin)
Windows process : inetinfo.exe
Type : Local RPC service
Named pipe : OLE59A762894D9643AD82C3408D3662

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0
Internet Information Service (IISAdmin)
Windows process : inetinfo.exe
Type : Local RPC service
Named pipe : INETINFO_LPC

Object UUID : 89deb52d-df73-4943-9f7a-adde466a6fca
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000514.00000001

Object UUID : c63b1e2d-0e59-4708-8658-897fdb31d6af
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000514.00000001

Object UUID : a3cb5b79-100a-4962-b3aa-112db3991661
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000514.00000001

Object UUID : f82e5568-237a-471e-9ed3-a25a7cd91236
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC00000514.00000001

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
```

Exhibit 13

```
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : dsrole

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : dsrole

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE53CE3EDA485D4FDA9AF120E0577A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
```

Exhibit 13

```
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE53CE3EDA485D4FDA9AF120E0577A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE53CE3EDA485D4FDA9AF120E0577A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service
Named pipe : OLE53CE3EDA485D4FDA9AF120E0577A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Local RPC service

Named pipe : AudioSrv
```

Using NetBIOS or SMB to retrieve information from a Windows host	ID	Port	Risk
Windows :: Nessus	110150	TCP:137	1

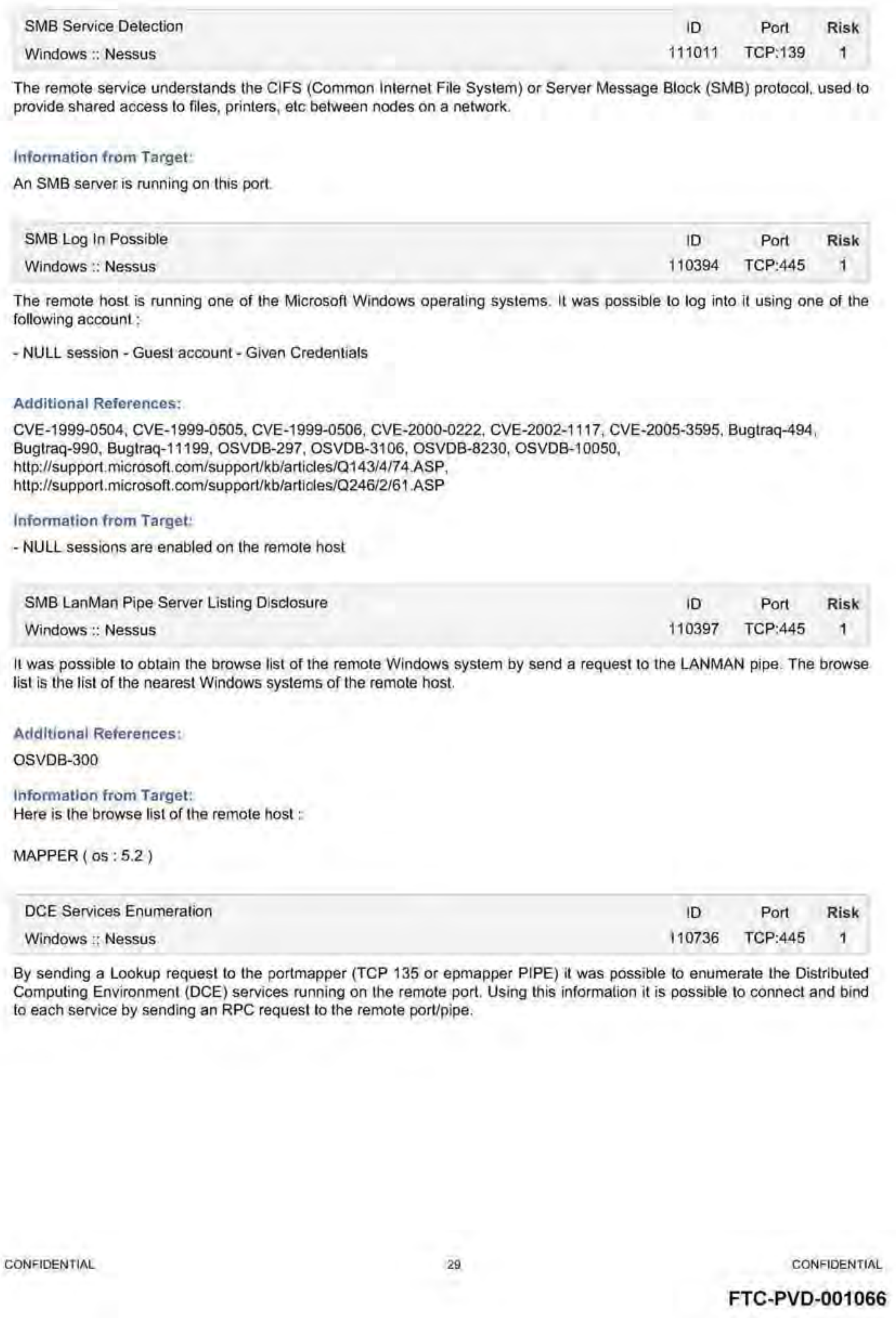
The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Information from Target:

```
The following 6 NetBIOS names have been gathered :

MAPPER = Computer name
WORKGROUP = Workgroup / Domain name
MAPPER = File Server Service
WORKGROUP = Browser Service Elections
WORKGROUP = Master Browser
__MSBROWSE__ = Master Browser

The remote host has the following MAC address on its adapter :

00:19:b9:d1:58:e9
```

Exhibit 13



SMB Service Detection	ID	Port	Risk
Windows :: Nessus	111011	TCP:139	1

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Information from Target:

An SMB server is running on this port.

SMB Log In Possible	ID	Port	Risk
Windows :: Nessus	110394	TCP:445	1

The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it using one of the following account :

- NULL session - Guest account - Given Credentials

Additional References:

CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595, Bugtraq-494, Bugtraq-990, Bugtraq-11199, OSVDB-297, OSVDB-3106, OSVDB-8230, OSVDB-10050,
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP,
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Information from Target:

- NULL sessions are enabled on the remote host

SMB LanMan Pipe Server Listing Disclosure	ID	Port	Risk
Windows :: Nessus	110397	TCP:445	1

It was possible to obtain the browse list of the remote Windows system by send a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Additional References:

OSVDB-300

Information from Target:

Here is the browse list of the remote host :

MAPPER (os : 5.2)

DCE Services Enumeration	ID	Port	Risk
Windows :: Nessus	110736	TCP:445	1

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Exhibit 13

Information from Target:

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \\PIPE\\ROUTER
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \\pipe\\trkwks
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \\PIPE\\srvsvc
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \\pipe\\keysvc
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \\PIPE\\W32TIME_ALT
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Unknown RPC service
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \\pipe\\tapsrv
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0
Internet Information Service (IISAdmin)
Windows process : inetinfo.exe
Type : Remote RPC service
Named pipe : \\PIPE\\INETINFO
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
```

Exhibit 13

```
Named pipe : \\PIPE\\lsass
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \\PIPE\\protected_storage
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
Named pipe : \\PIPE\\lsass
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
Named pipe : \\PIPE\\protected_storage
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \\PIPE\\atsvc
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \\PIPE\\atsvc
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \\PIPE\\atsvc
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \\PIPE\\atsvc
Netbios name : \\\\MAPPER

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d674a233-5829-49dd-90f0-60cf9ceb7129, version 1.0
Unknown RPC service
```

Exhibit 13

Annotation : ICF+ FW API
Type : Remote RPC service
Named pipe : \\PIPE\\wkssvc

Netbios name : \\\\MAPPER

SMB NativeLanManager Remote System Information Disclosure	ID	Port	Risk
Windows :: Nessus	110785	TCP:445	1

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Information from Target:

The remote Operating System is : Windows Server 2003 3790 Service Pack 2
The remote native lan manager is : Windows Server 2003 5.2

The remote SMB Domain Name is : MAPPER

SMB Service Detection	ID	Port	Risk
Windows :: Nessus	111011	TCP:445	1

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Information from Target:

A CIFS server is running on this port.

SMB registry can not be accessed by the scanner	ID	Port	Risk
Windows :: Nessus	126917	TCP:445	1

It was not possible to connect to PIPE\\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

SMB NULL Session Authentication	ID	Port	Risk
Windows :: Nessus	126920	TCP:445	1

The remote host is running Microsoft Windows, and it was possible to log into it using a NULL session (ie, with no login or password). An unauthenticated remote attacker can leverage this issue to get information about the remote host.

Additional References:

CVE-2002-1117, Bugtraq-494, http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP, http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

DCE Services Enumeration	ID	Port	Risk
Windows :: Nessus	110736	TCP:1025	1

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Exhibit 13

Information from Target:

The following DCERPC services are available on TCP port 1025 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 1025
IP : 64.190.124.7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 1025
IP : 64.190.124.7

DCE Services Enumeration	ID	Port	Risk
Windows :: Nessus	110736	TCP:1029	1

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Information from Target:

The following DCERPC services are available on TCP port 1029 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0
Internet Information Service (IISAdmin)
Windows process : inetinfo.exe
Type : Remote RPC service
TCP Port : 1029
IP : 64.190.124.7

SSL Cipher Suites Supported	ID	Port	Risk
Miscellaneous :: Nessus	121643	TCP:2002	1

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

Additional References:

http://www.openssl.org/docs/apps/ciphers.html

Exhibit 13

Information from Target:

```
Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}
```

Unknown Service Detection: HELP Request	ID	Port	Risk
Service Detection :: Nessus	111153	TCP:3306	1

This plugin is a complement of find_service1.nasl. It sends a HELP request to the remaining unknown services and tries to identify them.

Information from Target:

```
A MySQL server is running on this port
```

Exhibit 13

External Advisories

Some of the security threats discovered have external advisory sources for additional cross-reference information. To view the external advisory information, click on the reference number in the table below. Other web resources listed for the threat will be linked to as well.

ID	Risk	Description and References
110088	5	Anonymous FTP Writeable root Directory CVE-1999-0527, OSVDB-76, http://www.cert.org/advisories/CA-1993-10.html
118028	4	MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066) (uncredentialed check) CVE-2005-0048, CVE-2004-0790, CVE-2004-1060, CVE-2004-0230, CVE-2005-0688, Bugtraq-13124, Bugtraq-13116, OSVDB-4030, OSVDB-14578, OSVDB-15457, OSVDB-15463, OSVDB-15619, http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx
129345	3	MySQL Community Server < 5.1.23 / 6.0.4 Multiple Vulnerabilities CVE-2007-5969, CVE-2007-5970, CVE-2007-6303, CVE-2007-6304, Bugtraq-26765, Bugtraq-26832, OSVDB-42607, OSVDB-42608, OSVDB-42609, OSVDB-42610, http://bugs.mysql.com/32091, http://bugs.mysql.com/32111, http://bugs.mysql.com/29908, http://bugs.mysql.com/29801, http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html, http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html
112213	2	TCP/IP Sequence Prediction Blind Reset Spoofing DoS CVE-2004-0230, Bugtraq-10183, OSVDB-4030, IAVA-2004-A-0007, http://www.securityfocus.com/bid/10183/solution/
110079	2	Anonymous FTP Enabled CVE-1999-0497, OSVDB-69
110397	1	SMB LanMan Pipe Server Listing Disclosure OSVDB-300
110114	1	ICMP Timestamp Request Remote Date Disclosure CVE-1999-0524, OSVDB-94
121643	1	SSL Cipher Suites Supported http://www.openssl.org/docs/apps/ciphers.html
126920	1	SMB NULL Session Authentication CVE-2002-1117, Bugtraq-494, http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP, http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP
403092	1	Interesting Web Document Found OSVDB-3092
110394	1	SMB Log In Possible CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595, Bugtraq-494, Bugtraq-990, Bugtraq-11199, OSVDB-297, OSVDB-3106, OSVDB-8230, OSVDB-10050, http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP, http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP
135716	1	Ethernet card brand http://standards.ieee.org/faqs/OUI.html, http://standards.ieee.org/regauth/oui/index.shtml

Exhibit 13

Education

The Education report is written to provide a very high level explanation of network and information security. This report will also show some statistics about the need for security, dispel common myths about security, and define (in plain English) many of the terms used throughout this document.

This particular section is non-technical and is geared toward non-technical individuals, business management, and/or executives. For the stated audience, this report should be a prerequisite to the other reports in this document. If you are already familiar with Security documents, or if you are a technical professional, you may wish to simply skim this Education report. However, if you are a non-technical person, it is strongly recommended that you read this report.

What is Network and/or Information Security

Before you can understand the concept of network security, you must decide what security means to you and your company. Perhaps to you, feeling secure means knowing that you are safe from any outsider gaining access to your confidential files and private company information. If this is the case, use this policy to evaluate what goes on with your network because the same private information is also stored in your computer systems.

Network security simply means preventing unauthorized use of your computer network. Taking the necessary precautions to protect your network will help to keep unauthorized users, or hackers, from gaining access to your computer system or network. Network security can also assist you in detecting whether or not a hacker tried breaking into your system, and what damage, if any, was done.

When it comes to network security, most companies fall somewhere between two boundaries: complete access and complete security. A completely secure computer is one that is not connected to the network, not plugged in, and physically unreachable by anyone. Obviously, a machine like this does not serve much of a purpose in your office. On the other hand, a computer with complete access is very easy to use, requiring no passwords or authorization to provide information. Unfortunately, having a machine with complete access means anyone could access it. This could spell disaster for you and your organization.

Exhibit 13

Risk Factor Definitions

Security is a 100% impartial analysis company. The classifications shown below are therefore based on international and recognized industry standards.

Urgent Risk (Level 5)

Urgent Risk vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, remote execution of commands as a root or administrator user.

Critical Risk (Level 4)

Critical Risk vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as level 4 vulnerabilities.

High Risk (Level 3)

High Risk vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of 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).

Medium Risk (Level 2)

Medium Risk vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.

Low Risk (Level 1)

Low Risk vulnerabilities are informational, such as open ports.

Exhibit 13

Threat Family Definitions

AIX Local Checks

Local operating system and application level security checks for AIX.

Backdoors

Access to application files, system data, or confidential information.

Centos Local Checks

Local operating system and application level security checks for Centos.

CentOS Local Checks

CGI abuses

Cross-Site Scripting

Threats related to improper sanitation of untrusted input in web pages.

Database Services

Exploits in database servers, services, and configurations.

Debian Local Checks

Local operating system and application level security checks for Debian.

Denial of Service

Threats of DoS attacks exploits used to launch other DoS attacks.

DNS Services

Vulnerabilities with domain name servers and configurations.

Fedora Local Checks

Local operating system and application level security checks for Fedora.

Firewalls

Firewalls, Routers, SNMP

Threats or attack methods related to firewall and router devices and the SNMP protocol.

FreeBSD Local Checks

Local operating system and application level security checks for FreeBSD.

FTP Services

Vulnerabilities of FTP (file sharing) applications, servers, or services.

General

Exhibit 13

Gentoo Local Checks

Local operating system and application level security checks for Gentoo.

HP-UX Local Checks

Local operating system and application level security checks for HP-UX.

MacOS X Local Checks

Local operating system and application level security checks for MacOS X.

Mail Services

Threats dealing with e-mail server problems or exploits.

Mandriva Local Checks

Microsoft Bulletins

Local operating system and application level security checks for Microsoft Windows.

Misc.

Miscellaneous

Various threats and attacks that do not fit into any other family.

Netware

Problems with Netware operating systems, applications, and services.

Peer-To-Peer Services

Threats of exposed private data through file sharing services.

Port scanners

Red Hat Local Checks

Local operating system and application level security checks for Red Hat.

Remote File Access

Unauthorized access to files or data on your systems.

Remote Shell Access

Vulnerability of user or service-level accounts and information.

Service Detection

Tests for services, ports, and versions.

Slackware Local Checks

Local operating system and application level security checks for Slackware.

Solaris Local Checks

Local operating system and application level security checks for Solaris.

Exhibit 13

SuSE Local Checks

Local operating system and application level security checks for SuSE.

Ubuntu Local Checks

Local operating system and application level security checks for Ubuntu.

Unix

Problems, exploits, or attack methods related to UNIX systems or common UNIX services.

VMWare ESX Local Checks

Web Services

Problems exposed by web servers, configurations, or CGI scripts.

Windows

Problems with Windows operating systems, applications, and services.

Exhibit 13

Definitions of Technical Terms

ARIN
American Registry of Internet Numbers. This is the primary governing body that regulates Internet IP addresses. Other similar registries include APNIC and RIPE.

CGI
Common Gateway Interface. A standard structure and protocol for running external programs from a web server. For example, a program to process e-commerce credit card purchases would likely use CGI.

CVE / CAN
Common Vulnerabilities and Exposures / CANdidate. A dictionary that tracks information about known network and information security vulnerabilities.

DoS
Denial of Service. DoS is a specific type of network attack which can make servers and/or routers crash and typically results in a network outage.

DNS
Domain Name System/Service. A protocol used on the Internet for translating hostnames into Internet addresses. For example, DNS is the service that would translate www.google.com into the IP address 216.239.57.104. DNS is basically a phone book for the Internet.

Domain Name
Strings of alphanumeric characters used to name/identify computers, networks, and organizations on the Internet.

Exploit
A vulnerability in software or computer configurations that can be used for breaking security or otherwise attacking an Internet host over the network.

Family
The classification system used to determine the general category or type of service affected by a particular security threat. For example, security threats specific to Microsoft Windows systems would be classified in the "Windows" family in the security threats database.

Fingerprint
To identify by means of a distinctive mark or characteristic. For example, fingerprints are used to remotely identify which services, servers, operating systems, etc... that are running on any network.

Firewall
Any of a number of security schemes that prevent unauthorized users from gaining access to a computer network. Generally, a firewall is a hardware device installed on a network to help protect the network from hackers and attacks.

Hacker
A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. Many times the term is also used to describe a person who breaks into computer systems and/or networks.

Host
See Server.

IP Address
A numerical representation of a computer's address on the Internet.

MTA
Mail Transport Agent. The program running on a server to perform email functions and protocols. For example, when you send an email, your ISP's mail server uses an MTA to process the message.

Nessus
Open source security scanning engine used by most security professionals world-wide.

Network
An interconnected group of computers and electronic systems. A LAN is an example of a network. The Internet is another (albeit much more complex) example of a network.

Exhibit 13

Port

A computer's network interface is divided into several channels - each channel is called a "port." A port is used by specific hardware or software components to service requests on a network. For example, web servers typically use port number 80 to accept connections from users' web browsers. Generally, each computer has 65,535 unique ports.

Port Scan

The process of examining a group of ports on a computer to determine which ones are active. A port scan does not identify which applications/services are running on a computer, what any active ports are used for, or any security threats on the computer. It only determines which ports are active.

Protocol

A standard procedure for regulating data transmission between computers. For example, an email server uses a specific set of protocols so that anyone on the Internet can send email to anyone else on the Internet - regardless of which software or ISP either party is using.

Risk Factor

The classification system used to determine the severity or potential impact of a particular security threat.

Security Scan

The process of using various information security methodologies and techniques to audit the level of security for a computer, application, service, and/or network.

Security Threat

See Exploit.

Server

A computer that provides some service(s) to other computers that are connected to it via a network. For example, a web server provides web pages to your computer via the Internet.

Service

Work performed, or offered by, a server. For example, a web server offers the service of providing web pages to a web browser.

SSL

Secure Sockets Layer. A protocol designed to provide encrypted secure communications on the Internet. SSL is very commonly used to secure the transmission of e-commerce transactions. However, SSL does not provide any security for data after the initial transmission of the transaction.

TCP/IP

Transmission Control Protocol / Internet Protocol. A suite of data networking and communications protocols for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

Virus

A rogue computer program that searches out other programs and infects them by embedding a copy of itself in them, so that they become Trojan horses. When these programs are executed, the embedded virus is executed too, thus propagating the infection. This normally happens invisibly to the user.

Vulnerability

See Exploit.

VPN

Virtual Private Network. The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

Whois

An Internet directory service for looking up information on a remote server. Whois is commonly used to lookup information about people, companies, IP addresses, computers, and domain names.

Exhibit 13

Exhibit 14

In the Matter of:

LabMD, Inc.

January 24, 2014
Patrick Howard

Condensed Transcript with Word Index

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

Exhibit 14

CONFIDENTIAL – REDACTED IN ENTIRETY

Exhibit 15

In the Matter of:

LabMD, Inc.

February 27, 2014
Allen Truett

Condensed Transcript with Word Index

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

Exhibit 15

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 16

In the Matter of:

LabMD, Inc.

February 5, 2014
Alison Simmons

Condensed Transcript with Word Index

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

Exhibit 16

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 17

Report of Rick Kam, CIPP/US

In the Matter of LabMD

FTC Complaint #1023099, Docket #9357

March 18, 2014

Exhibit 17

Table of Contents

Exhibit 17

Executive Summary

Federal Trade Commission staff has retained me as an expert witness in the Commission's administrative litigation against LabMD. Complaint Counsel has asked me to assess the likely risk of injury, particularly from medical identity theft, to consumers caused by the unauthorized disclosure of their sensitive personal information. This document is a statement of my opinions and contains the bases and reasons for my conclusions. It includes the following information:

- Overview of my credentials and qualifications.
- Overview of the impact of identity crimes from the perspective of consumers affected by the unauthorized disclosure of sensitive personal information.
- Analysis of the potential harm[1] and risk of harm from medical identity theft to consumers whose sensitive personal information was disclosed without authorization.

I. Introduction

My name is Rick Kam, president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. ID Experts is based in Portland, Oregon. Since 2003, leading healthcare, financial, and educational organizations, and state and federal government agencies have relied on ID Experts to help them respond to unauthorized disclosures of sensitive personal information. I have had the opportunity to work on data breach incidents as part of ID Experts' incident response team. ID Experts has managed hundreds of incidents, protecting millions of affected individuals and restoring the identities of thousands of identity theft victims. Within the healthcare industry, I have worked with organizations ranging in size from individual providers and small clinics to large hospital systems and health insurance companies. ID Experts is recognized as an industry leader, protecting consumers from the harms caused by the unauthorized disclosure of their sensitive personal data.

My expertise includes:

- Identifying and remediating the consequences of identity theft and medical identity theft for consumers whose sensitive personal information was compromised.

[1] The term "injury" is from the FTC complaint and is used interchangeably with the term "harm."

Exhibit 17

- Helping organizations develop policies and solutions to address the growing problem of safeguarding sensitive personal information.

Based on my unique experience at ID Experts, I lead and participate in several cross-industry data-privacy working groups, resulting in the publication of industry white papers. I regularly speak at conferences and on webinars; work with other privacy and security experts to contribute articles, including a monthly guest article in *Government Health IT*; and offer commentary to privacy, breach risk, and information technology (IT) publications.

Affiliations and Organizations

As a privacy professional, I actively work on initiatives that focus on data privacy to protect consumers and their sensitive personal information, and I belong to or have belonged to the following organizations:

- Chair of PHI Protection Network (PPN), an interactive network of privacy professionals focused on expediting the adoption of best practices to protect sensitive personal medical information. (2012 - present)

- Chair of The Santa Fe Group Vendor Council ID Management Working Group, which published *Victims' Rights: Fighting Identity Crime on the Front Lines,* February 2009. This white paper explores trends in identity crimes, the victim's experience, and proposes a victim's "bill of rights." (2008 - 2012)

- Chair of the American National Standards Institute (ANSI) Identity Management Standards Panel "PHI Project," a seminal research effort to measure financial risk and implications of data breach in healthcare, led by the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with the Shared Assessments Program and the Internet Security Alliance (ISA). The "PHI Project" produced *The Financial Impact of Breached Protected Health Information*. (2011 - 2012)

- Co-Chair of three other cross-industry working groups that published whitepapers on assessing cyber and data breach risks. The reports include: *IDSP Workshop Report: Measuring Identity Theft*; *The Financial Management of Cyber Risk: An Implementation Framework for CFOs;* and *The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*. (2007 - 2012)

- Contributor to the Research Planning Committee for the University of Texas Center for Identity, which focuses on identity management and identity theft risk mitigation best

Exhibit 17

practices. ID Experts provided case studies of identity crimes to an analytical repository of identity threats and counter measures called *Identity Threat Assessment and Prediction* (ITAP). (2009 - present)

- Member of the International Association for Privacy Professionals (IAPP), the most comprehensive, member-based privacy community and resource. I maintain a Certified Information Privacy Professional CIPP/US certification for data privacy. (2010 - present)

- Member of Healthcare Information and Management Systems Society (HIMSS), a global, member-based non-profit focused on the betterment of healthcare information technology. (2010 - present)

- Member of the Health Care Compliance Association, (HCCA), a member-based non-profit that provides training, certification and resources in support of ethics and regulatory compliance in healthcare. (2011- present)

- Founding member of the Medical Identity Fraud Alliance (MIFA), a group of over 40 private and public industry members in the fight against medical identity theft and medical fraud. (2013 - present)

I have attached a copy of my CV, which fully describes my background and qualifications, and includes a list of my publications over the last 10 years (see Appendix A).

Compensation

The FTC has engaged me as an expert witness in support of its complaint against LabMD. The compensation for this work is $350 per hour, and this report and my testimony are based on the experience outlined in this section, a literature review (see Appendix B), and documents I received from the FTC.

II. Summary of the FTC's Request for Expert Opinion

The Federal Trade Commission has asked me to assess the risk of injury to consumers caused by the unauthorized disclosure of their sensitive personal information. For the purposes of my analysis, I have assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks.

Exhibit 17

FTC Documents for Analysis

I have based my analysis on my experience as outlined in Section I of this report, a literature review (see Appendix B), and the documents that I received and reviewed from the FTC, which are listed here.

Documents related to the P2P Disclosure

- **P2P Insurance Aging file (insuranceaging_6.05.071.pdf):** This is the 1,718-page file Tiversa discovered on a peer-to-peer (P2P) network that contained consumer data from the LabMD Insurance Aging Report with roughly 9,300 records. The data elements included in this file are:
  - First and last names, and middle initials
  - Dates of birth
  - Nine-digit Social Security numbers (SSNs)
  - Health insurance provider numbers, names, addresses, and phone numbers
  - Current Procedural Terminology (CPT) Codes: Uniform set of codes defined by the American Medical Association to describe medical, surgical, and diagnostic services.
  - Billing dates and amounts

- **Transcript of the deposition of Robert Boback, CEO of Tiversa, dated November 21, 2013, with supporting exhibits.**

- **Transcript of the deposition of Alison Simmons, former LabMD IT employee, dated February 5, 2014, with supporting exhibits.**

- **Transcript of the deposition of Eric Johnson, Dean of the Owen Graduate School of Management at Vanderbilt University, dated February 18, 2014, with supporting exhibits.**

- **Transcript of the deposition of Michael Daugherty, President and CEO of LabMD, dated March 4, 2014.**

Documents related to the Sacramento Disclosure

- **Day Sheets from LabMD (Sacramento LabMD-Documents.pdf):** These are documents the Sacramento Police Department found on October 5, 2012, during an arrest of two individuals who pleaded “no contest” to identity theft charges. The Day Sheets contain approximately 600 records with first and last names, and middle initials; nine-digit Social Security numbers; and billing dates and amounts.

Exhibit 17

- **Nine (9) personal checks and one (1) money order from patients of LabMD (Sacramento LabMD-Documents.pdf):** The Sacramento Police Department also found these documents on October 5, 2012, during the same arrest. Information on the checks include: first and last names, and middle initials; addresses; bank routing and account numbers; and signatures. There are also handwritten notes with four of the personal checks with what appear to be SSNs, check numbers, and amounts.

- **"Sacrementoresults7" spreadsheet:** It contains an analysis by the FTC of the Social Security numbers found in the Day Sheets. The FTC used the Thomson Reuters CLEAR database for this analysis. This spreadsheet shows multiple instances of SSNs that are being, or have been, used by people with different names, which may indicate that identity thieves used these SSNs.

- **Transcript of the deposition of Detective Karina Jestes, dated December 17, 2013, with supporting exhibits.**

- **Transcript of the deposition of Kevin Wilmer, FTC investigator, dated February 25, 2014.**

- **Transcript of the deposition of Michael Daugherty, President and CEO of LabMD, dated March 4, 2014.**

- **Breach notification letter from LabMD to Peter Cuttino, letter dated March 27, 2013.**

- **Breach notification letter from LabMD to James Hayes, letter dated March 27, 2013.**

- **FTC Consumer Sentinel Network contact records (Norris and Cuttino.pdf).**

- **FTC-LABMD-003914 to 3915:** 3/27/13 letter from LabMD regarding personal information that "may have been compromised."

- **FTC-LABMD-003910 to 3911:** 12/6/13 letter from LabMD regarding credit monitoring.

Other Documents Related to the FTC Investigation

- **2010.02.24 Ellis Letter to the FTC**
- **2010.06.04 Ellis Letter to the FTC**
- **2010.07.16 Ellis Letter to the FTC**
- **2010.08.30 Ellis Letter to the FTC**
- **2011.05.16 Rosenfeld Letter to the FTC**

Exhibit 17

- **2011.05.31 Rosenfeld Letter to the FTC**
- **2011.07.12 Rosenfeld Email to the FTC**
- **FTC-MID-000012:** 1/6/14 letter regarding LabMD not "accepting new specimens."
- **FTC Complaint in the Matter of LabMD**
- **Protective Order Governing Discovery of Material.pdf**
- **LabMD's Objections to and Responses to Complaint Counsel's Requests for Admission, dated March 3, 2014**
- **LabMD's Responses to Complaint Counsel's Interrogatories and Discovery Requests, dated March 3, 2014**

III. Summary of Conclusions

As consumers, we place trust in the organizations that hold our most sensitive personal information: Social Security numbers, financial data, and our medical history, to name a few. We have confidence that they will protect this information from unauthorized disclosure.

Once a consumer's sensitive personal data is disclosed without authorization, that consumer has no control over who accesses this information, thus becoming vulnerable to identity fraud, identity theft, and medical identity theft. These crimes can damage a consumer's economic well-being and reputation, and even risk his or her health. Medical identity theft can be especially difficult to resolve because it is impossible to make a victim's personal medical history private again.

In Sections V and VI of this report, I provide an overview of the impact of identity crime, with an emphasis on medical identity theft, and illustrate the possible harm to victims of these crimes. Then, based on that information, the FTC-provided documents, the literature review (see Appendix B), and my own expertise and experience, I provide my analysis of the LabMD case, specifically:

- That consumers have no way of knowing about certain unauthorized disclosures of their sensitive personal information, including medical information, thus putting them at risk of possible harms from identity crimes, including medical identity theft.

- That use of a consumer's SSN by other people with different names is an indication that identity thieves may have used the consumer's SSN.

- That LabMD's failure to employ reasonable and appropriate measures to prevent unauthorized access to consumers' personal information is likely to cause substantial harm, including harm stemming from medical identity theft.

Exhibit 17

Summary of LabMD Analysis

In my opinion, LabMD's failure to provide reasonable and appropriate security for sensitive personal information, including medical information, is likely to cause substantial injury to consumers and puts them at significant risk of identity crimes. The following is a summary of my analysis of likely risks of harm from identity theft and medical identity theft to the approximately 10,000 consumers affected by the P2P and Sacramento disclosures. Apart from these two incidents, I also believe that LabMD's failure to provide reasonable and appropriate security for the more than 750,000 consumers' personal information maintained on its computer networks creates a risk of unauthorized disclosure of this information. These unauthorized disclosures and the failure to provide reasonable and appropriate security are likely to cause substantial harm to these consumers.

P2P Disclosure

- Approximately 9,300 consumers from the May 2008 unauthorized disclosure are at significant risk of harm from identity crimes.

- LabMD did not notify the 9,300 consumers whose personal information was contained in the 1,718-page P2P Insurance Aging file that Tiversa discovered on February 5, 2008. Robert Boback indicated in his testimony on November 21, 2013, that this file was found on peer-to-peer networks. He indicated that at four of the IP addresses on which Tiversa found the 1,718-page P2P Insurance Aging file, Tiversa also found unrelated sensitive consumer information that could be used to commit identity theft, including passwords, tax returns, account numbers, and Social Security numbers.

- These 9,300 consumers have had no opportunity to mitigate the risk of harm because LabMD, which has known about the unauthorized disclosure of their personal information since May 2008, has not notified them of this disclosure. Even if LabMD had provided notice, consumers would still remain at risk of harm from identity crimes since this unauthorized disclosure included Social Security numbers and health insurance numbers, which can be used to commit identity crimes over an extended period of time.

- There is a significant risk of reputational damage for 3,000 or more consumers from the unauthorized disclosure of sensitive medical information, specifically diagnostic codes indicating tests for prostate cancer, herpes, hepatitis, HIV, and testosterone levels.

Exhibit 17

Sacramento Disclosure

The approximately 600 consumers whose personal information was contained in the LabMD documents found in the hands of Sacramento identity thieves are at risk of harm from identity crimes. In March 2013, LabMD notified these consumers about the incident. LabMD's March 2013 notification gave the affected consumers an opportunity to mitigate some risks of harm. However, consumers receiving notification of data breaches are not immune to identity crime, and they remain at risk of harm from identity crimes.

Consumer Harm from Failing to Provide Reasonable and Appropriate Security

There is a risk of harm to consumers when a company fails to protect sensitive personal information. Apart from the P2P and Sacramento incidents, I also believe that LabMD's failure to provide reasonable and appropriate security for all of its consumers' personal information maintained on its computer networks increases the risk of unauthorized disclosure of this information—likely causing substantial harm to these consumers. This harm often takes the form of identity crimes, including identity theft, identity fraud, and medical identity theft.

IV. Identity Crime: An Overview

This section provides a short overview of the different types of identity crimes—identity theft, identity fraud, and medical identity theft.

Definition of Identity Theft and Identity Fraud

Identity theft occurs when someone uses another person's identity without his or her permission. This could include using another person's name, address, date of birth, Social Security number, credit card and banking information, drivers license, or any combination of these types of personal identifiers to impersonate them. Collectively, this type of information is known as personally identifiable information, or PII.

Identity fraud, for purposes of this report, is the unauthorized use of some portion of another person's information to achieve illicit financial gain. This definition is consistent with that used by Javelin Strategy and Research. In my role at ID Experts, I have managed teams working with thousands of identity theft and identity fraud victims, helping them pinpoint the issues identity thieves caused and working to expunge any negative records created by the identity thieves. Identity thieves can use PII to commit numerous crimes, as illustrated by this list of types of theft that teams working under my supervision have helped consumers resolve:

Exhibit 17

- Using another person’s SSN to create credentials such as fake drivers licenses and birth certificates to perpetrate and legitimize identity fraud.
- New accounts for major credit cards, various retail store cards, and mail-order accounts.
- Takeover of legitimate victim accounts resulting in fraudulent purchases, including goods and services.
- New bank accounts, including checking/savings/investment, resulting in several bank accounts reported to collections.
- Check counterfeiting and forgery.
- Fraudulent tax returns causing victims not to receive their refunds or to seem to owe extensive funds.
- Payday loan fraud reported to collections and other agencies.
- New auto financing accounts for multiple vehicle purchases. These vehicles were then not registered, incurring fees to the victim and making it impossible for them to legitimately register their own vehicles, while the thief sold the fraudulently purchased vehicles.
- Fake drivers licenses created to perpetrate and legitimize fraud, further complicating the dispute process.
- Employment fraud, in which an individual fraudulently works in another state and reports the wages, causing the victim to receive tax notices for non-payment and have difficulty filing legitimate tax returns.
- Merchant processing accounts set up under fake businesses to take credit card payments.

According to the *2014 Identity Fraud Report* by Javelin Strategy and Research, nearly one in three data breach victims (30.5%) also fell victim to identity fraud in 2013.[2]

Definition of Medical Identity Theft

Medical identity theft occurs when someone uses another person’s medical identity to fraudulently receive medical services, prescription drugs and goods, as well as attempts to fraudulently bill private and public health insurance entities.

A person’s medical identity is comprised of a number of personal data elements. The teams I have supervised at ID Experts have worked on hundreds of healthcare data breaches, in which many of the following data elements were affected:

- Name
- Medical record number
- Health insurance number

[2] *2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends*, p. 29, February 2014, by Javelin Strategy & Research.

Exhibit 17

- Other demographics (which may include address, phone number)
- Charge amounts for services
- Social Security number
- Medicare number (which contains a person's nine-digit SSN)
- Date of birth
- Financial account information
- Patient diagnosis [i.e., International Classification of Diseases (ICD), and Current Procedural Terminology Codes (CPT)]

Medical identity theft is a serious problem, affecting an estimated 1.84 million Americans.[3]

Identity Thieves and Identity Fraud

It may take months or years for a consumer to learn that his or her sensitive personal information was disclosed without authorization and misused to commit an identity crime. This is due, in part, to identity criminals committing a wide variety of identity fraud, some of which may be difficult for the consumer to detect. The teams I have managed at ID Experts work with victims who, in many cases, have several identity fraud issues. A number of the victims we have worked with continue to be harmed, since identity thieves will resell their sensitive personal information to other identity thieves, thus perpetuating the harms for years.

In 2007, Utica College did a study using 517 actual identity theft cases investigated by the U.S. Secret Service.[4] The study did not depend on self-reported victim data. The purpose of the study was to understand the nature, perpetrators, and case characteristics of identity crimes. It found the most significant motive for identity thieves to commit identity fraud is for personal financial gain (see Table 1 below).

[3] *2013 Survey on Medical Identity Theft*, p. 2, September 2013, by Ponemon Institute. From http://medid-fraud.org/2013-survey-on-medical-identity-theft/.

[4] *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, p. 38, October 2007, by Center for Identity Management and Information Protection, Utica College. From http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf.

Exhibit 17

Table 1: Motivating Factors for Committing Identity Theft or Fraud

Motive	Number	Percentage
Use stolen ID to obtain and use credit	228	45.3%
Use stolen ID to procure cash	166	33%
Use stolen ID to conceal actual identity	114	22.7%
Use stolen ID to apply for loans to buy vehicles	105	20.9%
Use stolen ID to manufacture and sell fraudulent IDs	39	7.7%
Use stolen ID to obtain cell phones and services	23	4.6%
Use stolen ID to gain government benefits	19	3.8%
Use stolen ID to procure drugs	11	2.2%

V. Impact of Identity Crimes on Victims

This section highlights the range of harms that can befall victims of the various forms of identity crimes, with an emphasis on medical identity theft. Here are just a few examples of the challenges and frustrations a typical identity crime victim may experience based on my work at ID Experts:

- The victim may have to deal with a dizzying array of businesses and government institutions. It is not uncommon for an identity thief to establish as many as five fraudulent accounts. In healthcare, for example, a visit to the emergency room would result in several bills (i.e. ambulance, lab, emergency room, doctors). Victims would need to contact each of these entities to dispute fraudulent charges and close these accounts. In many cases this entails following up and submitting copies of a police report, ID theft affidavit, proof of residence, and identification. The victim may have to contact the entity several times to ensure his or her accounts are corrected and all negative records created by the identity thieves are expunged.

Exhibit 17

- Some local police departments won't accept a police report from an identity theft victim. In our experience, we are aware that taking police reports related to identity crimes works against department crime metrics, which may be a disincentive for police to help victims.

- There is no central "medical identity bureau" where a consumer can set up a fraud alert, like they can with the credit bureaus. He or she has no way to notify healthcare providers or payers, or receive consumer alerts, which are part of credit monitoring services. As a result, identity thieves can continue to use a consumer's medical identity to commit identity crimes.

- If criminal acts are committed under a stolen identity, the first news a victim often has of the theft may be when he or she is arrested. The identity thief's arrest record may also show up in background checks of a victim, affecting things such as passing security clearances, receiving a drivers license, and taking advantage of career opportunities.

- If a victim's checkbook is stolen, this usually means closing out the old account, opening a new one, and filing a police report in case merchants were cheated with bad checks. Some financial institutions won't reimburse all fraud losses for checking or savings accounts until they are confirmed as fraudulent, which may impact a consumer's ability to pay his or her bills.

- Identity thieves submitting fraudulent tax returns is another growing problem affecting approximately 1.8 million consumers.[5] Tax identity theft typically prevents victims from being able to successfully file their tax returns and obtain refunds.[6] The delay can extend, in some cases, as long as six months.[7] This delay materially affects victims' cash flow.

- Many hospitals and clinics do not have staff training or internal processes to help victims of identity theft and medical identity theft. Consumers may not get help or a response unless they can get to a manager, such as the organization's chief medical officer or compliance officer.

[5] "Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Returns," No. 2013-40-122 (Sept. 20, 2013) (public) p. 1, by Treasury Inspector General. From http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.html.

[6] "Tips for Taxpayers, Victims about Identity Theft and Tax Returns," by Internal Revenue Service, January 2013. From http://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers,-Victims-about-Identity-Theft-and-Tax-Returns.

[7] Ibid.

Exhibit 17

- The victim of medical identity theft may have the integrity of their electronic health record compromised if the health information of the identity thief has merged with that of the victim. The resulting inaccuracies may cause serious health and safety risks to the victim, such as the wrong blood type or life-threatening drug allergies.

Financial Harm from Medical Identity Theft

The *2013 Survey on Medical Identity Theft* by Ponemon Institute found that 36 percent of medical identity theft victims incurred an average of $18,660 in out-of-pocket expenses.[8] These costs stem from medical identity theft and include: 1) reimbursement to healthcare providers for services received by the identity thief; 2) money spent on identity protection, credit counseling, and legal counsel; and 3) payment for medical services and prescriptions because of a lapse in healthcare coverage.[9]

Other Harms from Medical Identity Theft

In addition to out-of-pocket costs, victims spent a significant amount of time resolving the problems caused by medical identity theft. According to the Ponemon Institute survey, the amount of time it takes to resolve the crime can discourage victims of medical identity theft from even trying to fix the problem. This is due, in part, because healthcare organizations believe they cannot release medical records that include the identity thief's sensitive personal information to a victim of medical identity theft. For those victims who did try, 36 percent of respondents say it took nearly a year or more working with their healthcare providers or insurers to resolve the crime, and 48 percent say "the crime is still not resolved."[10]

Another problem is health insurance. The Ponemon survey found that 39 percent of medical identity theft victims lost their healthcare coverage.[11] Most life and health insurance organizations subscribe to organizations such as the Medical Information Bureau, which is an insurance consumer reporting agency that maintains a database of medical information to help insurers determine risk and insurance rates for individual consumers.[12] A medical identity theft victim who has been diagnosed with and received prescriptions for conditions that are costly to treat, like cancer or HIV, could possibly lose life or health insurance coverage.

[8] Ponemon Institute 2013 Survey on Medical Identity Theft, p. 5.

[9] Ponemon Institute 2013 Survey on Medical Identity Theft, p. 5.

[10] Ponemon 2013 Survey on Medical Identity Theft, p. 12.

[11] Ponemon 2013 Survey on Medical Identity Theft, p. 10.

[12] The Facts about the Medical Information Bureau (MIB). From http://www.mib.com/facts_about_mib.html.

Exhibit 17

The Ponemon survey on medical identity theft breaks down other harms of medical identity theft to victims including serious health-related risks, loss of confidence in their medical care provider, and more. Using statistics from the Ponemon study,[13] Table 2 below illustrates the health risks to victims of medical identity theft:

Table 2. Other Harms from Medical Identity Theft	**Ponemon Percentage of Medical Identity Victims**
Misdiagnosis of Illness*+	15%
Delay in Receiving Medical Treatment*+	14%
Mistreatment of Illness*+	13%
Wrong pharmaceuticals prescribed*+	11%

**Consequences as a result of inaccuracies in health records.*
+ Respondents were permitted two choices for this portion of the survey.

Potential for Reputational Harm from Medical Identity Theft

Reputational harm can occur from the loss of sensitive personal health information. Medical identity theft victims who may have sexually transmitted diseases are particularly sensitive to having their condition disclosed. Consumers diagnosed with cancer may feel similarly stigmatized. There have also been cases of criminals trying to extort money in exchange for not disclosing sensitive information. Two cases were reported in 2008, in which criminals tried to extort money from Express Scripts and Medical Excess LLC, a subsidiary of AIG, in return for not disclosing health records.[14]

[13] Ponemon 2013 Survey on Medical Identity Theft, p. 8.

[14] "Express Scripts Data Breach Leads to Extortion Attempt," by Sarah Rubenstein, November 7, 2008, *Wall Street Journal* Health Blog, http://blogs.wsj.com/health/2008/11/07/express-scripts-data-breach-leads-to-extortion-attempt/.

Exhibit 17

VI. Analysis of Risk of Harm from LabMD's Failure to Protect Consumer Data

In this section, I analyze the risk of harm from medical identity theft to consumers resulting from LabMD's failure to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks. Specifically, I identify the possible harm to the approximately 10,000 consumers known to be affected by LabMD's unauthorized disclosures of sensitive personal information. Given the specific circumstances of this case, in which LabMD's sensitive consumer data was found in the hands of known identity thieves and the fact that this sensitive consumer data was found on P2P networks as recently as November 2013—and may still exist on these networks—these estimates should be viewed as a floor versus universe of potential harms that could befall the 10,000 affected consumers.

I also explain how, irrespective of these two incidents, LabMD's failure to provide reasonable and appropriate security for more than 750,000 consumers' personal information maintained on its computer networks creates a risk of unauthorized disclosure of this information, thus causing a likelihood of substantial harm to consumers.

Consumers' Ability to Avoid Possible Harms

A consumer cannot know about the security practices of every company that collects or maintains his or her personal information. As a result, states have enacted data breach notification laws (see Appendix C for a list of the state data breach notification laws in effect in May 2008). Generally, notifications are intended to alert affected consumers of a breach so that they can take actions to reduce their risk of harm from identity crime. Without notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information.

It should be noted that breach notification doesn't completely eliminate the risk of harm to consumers from identity crimes. The fact that a consumer's sensitive personal information has been disclosed significantly increases the risk of harm—especially if this information is in the possession of criminals. Javelin Research finds that almost one in three data breach victims in 2013 fell victim to identity fraud in the same year.[15]

For my analysis I used the following four factors to examine the likely risk of harm to consumers from the unauthorized disclosure of their sensitive personal information:

[15] Javelin 2014 Identity Fraud Report, p. 8.

Exhibit 17

1. The nature and extent of the sensitive personal information involved, including the types of identifiers and the likelihood of re-identification. In other words, could the disclosed consumer data elements be used to facilitate identity theft, identity fraud, and medical identity theft? Was sensitive personal data part of the unauthorized disclosure (e.g., name, medical records, health insurance number, diagnostic codes)?

2. The unauthorized person who used the protected health information or to whom the disclosure was made. For instance, was this an employee disclosing the information to another employee, which poses a low risk, versus to an unauthorized individual not associated with that entity, be it another consumer, business, identity thief, etc.?

3. Whether the sensitive personal information was actually acquired or viewed. An example: Was the information stored on a secure encrypted device such as a laptop or storage drive, or were they paper health records left on a public bus and viewed by others?

4. The extent to which the risk to the protected health information has been mitigated. For instance: Were copies of sensitive information destroyed during its recovery from unauthorized parties, or is the data still available for others to misuse?

Analysis of the P2P Disclosure (9,300 records)

According to the materials supplied by the FTC, Tiversa alerted LabMD of the unauthorized disclosure of the P2P Insurance Aging file that contained 9,300 consumer records in May 2008. The compromised data included:

- First and last names, and middle initials
- Dates of birth
- Nine-digit Social Security numbers
- Health insurance provider numbers, names, addresses, and phone numbers
- Current Procedural Terminology (CPT) diagnostic codes
- Billing dates and amounts

I analyzed these data elements looking at the first risk factor, specifically the nature and extent of the information disclosed. Approximately 9,300 consumers' sensitive data was found in a LabMD document available on a P2P network on February 5, 2008, in clear text, according to Robert Boback's testimony. The disclosure of names with corresponding Social Security numbers, health insurance provider numbers, and CPT diagnostic codes pose a greater risk of various identity crimes.

Exhibit 17

The second and third risk factors consider to whom the disclosure was made and whether the information was acquired and viewed. In his testimony, Boback said that the P2P Insurance Aging file was found at four IP address along with unrelated sensitive consumer information that could be used to commit identity theft. Boback also testified sensitive consumer information in the P2P file could be available to anyone who had access to the peer-to-peer network. He also stated that law enforcement had apprehended someone suspected of identity theft or fraud using one of the IP addresses.

The fourth risk factor is the extent to which the risk to a consumer's personal information has been mitigated. According to Boback's testimony, the P2P Insurance Aging file was first found on the peer-to-peer network on February 5, 2008, at IP address 68.107.85.250. It was found again on November 5, 2008, at IP address 173.16.83.112; again on April 7, 2011, at IP address 201.194.118.82; and yet again on June 9th in 2011, at IP address 90.215.200.56. Boback also said Tiversa searched for the file in preparation for his testimony on November 21, 2013, and still found the file available on the P2P network. LabMD did not mitigate the risk of identity crimes created by this unauthorized disclosure by notifying consumers. In my experience, a significant number of these consumers have or could still fall victim to identity crimes since they have no way of independently knowing that LabMD disclosed their information without authorization almost 6 years ago. This unauthorized disclosure puts the affected consumers at a significantly higher risk of identity crimes than the general public.

Harm from P2P Disclosure

Estimated Financial Out-of-Pocket Cost to Victims of Medical Identity Theft

According to the findings from the 2013 Survey on Medical Identity Theft by Ponemon Institute, 0.0082 is the estimated base rate for medical identity theft in the U.S.[16] This represents the proportion of consumers who indicated that they were medical identity theft victims, as drawn from a representative panel of 5,000 adult-aged U.S. consumers.[17]

Therefore:

9,300 breached records x 0.0082 = 76, the estimated number of victims for medical identity theft.

The Ponemon study also found that 36 percent of victims of medical identity theft paid an average of $18,660 in out-of-pocket costs.

[16] Ponemon 2013 Survey on Medical Identity Theft, p. 2.

[17] Ponemon 2013 Survey on Medical Identity Theft, p. 27.

Exhibit 17

Therefore:

9,300 breached victims x 0.0082 base rate x 0.36 = 27 potential victims who would have to pay the average of $18,660 in out-of-pocket costs. Consumers' out-of-pocket costs would exceed $500,000.

Estimation of "Other" Injury from Medical Identity Theft

As discussed in Section V, medical identity theft and identity fraud have the potential to cause "substantial injury" to consumers in ways that are not directly related to finances. And as also mentioned above, LabMD's failure to notify the 9,300 individuals whose information is in the P2P Insurance Aging file potentially puts these consumers' health and safety at risk.

Table 3 below estimates the number of these consumers who could experience other kinds of harm.[18]

Table 3. Projected Number of Victims Suffering "Other Harms" from Medical Identity Theft

"Other Harms" from Medical Identity Theft	Ponemon % of Medical Identity Victims	Projected Number of Victims**
Misdiagnosis of Illness*+	15%	11
Delay in Receiving Medical Treatment*+	14%	11
Mistreatment of Illness*+	13%	10
Wrong pharmaceuticals prescribed*+	11%	8
Loss of health insurance coverage	39%	30

**Consequences as a result of inaccuracies in health records.*
+ Respondents were permitted two choices for this portion of the survey.
*** Calculation for number of possible victims is number of medical records (9,300) x 0.0082 Ponemon percentage of medical identity theft victims x Ponemon "% other harm."*

[18] Ponemon 2013 Survey on Medical Identity Theft, pp. 8,10.

Exhibit 17

Reputational Injury from Medical Identity Theft

In addition to SSNs and health insurance information, some of the most sensitive medical information disclosed by LabMD are the CPT codes indicating various tests that had been performed. (For an analysis of each CPT code included in the 1,718-page P2P Insurance Aging file, please see Appendix D.) The consumers identified in this file had various medical tests performed, as indicated by the CPT codes. Several of the CPT codes indicate tests for the presence of prostate cancer, testosterone levels, or STDs—specifically HIV, hepatitis, and herpes.

- There were 3,195 instances of CPT code 84153; 548 instances of CPT code 84154; and 109 instances of CPT code G0103. These CPT codes describe tests for "prostate specific antigen"—an indication of possible prostate cancer. More than 3,000 consumers had these CPT codes linked to their name.
- There were 134 instances of CPT code 84402 and 435 instances of CPT code 84403, which test for testosterone levels. Testosterone results can be used to evaluate men for testicular dysfunction. In men, low levels of testosterone may cause reduced fertility or lack of libido. More than 400 consumers had these CPT codes linked to their name.
- Nineteen (19) consumers had one or more of the following CPT codes, indicating tests for herpes: 86694, 86695, and 86696.
- Six consumers (6) had one or more of these CPT codes, indicating tests for hepatitis B or C: 86705 and/or 86706.
- There were 13 instances of CPT code 86689, which indicates a test for HIV.

Testing for these sensitive medical conditions does not necessarily indicate a diagnosis. However, disclosure of the fact that the tests were performed could cause embarrassment or other negative outcomes, including reputational harm and changes to insurance for these consumers, including life, health, and disability insurance. Once this health data is disclosed, it is impossible to restore the consumers' privacy.

Analysis of Sacramento Disclosure (~600 Records on Day Sheets, 9 Personal Checks, 1 money order)

The Sacramento Police Department discovered sensitive personal information in the possession of known identity thieves, including 40 pages of Day Sheets with approximately 600 records, and nine personal checks and one money order made out to LabMD. The compromised data contained on the LabMD Day Sheets included:

- First and last names, and middle initials
- Nine-digit Social Security numbers

Exhibit 17

- Billing dates and amounts

The compromised data contained on the nine checks included:

- First and last names, and middle initials
- Address
- Nine-digit Social Security numbers
- Bank routing and account numbers (on checks)
- Amounts
- Signatures
- Handwritten comments that appear to be SSNs, check numbers, and amounts

I analyzed these data elements using the first risk factor: the nature and extent of sensitive personal information disclosed. This incident disclosed sensitive consumer information, specifically names, nine-digit SSNs, and bank routing and account numbers on the nine checks. This sensitive personal information could be used to commit identity theft and identity fraud.

The Sacramento Police Department found 40 pages of LabMD Day Sheets and nine checks during an arrest on October 5, 2012, in the possession of two individuals who pleaded "no contest" to identity theft. While Detective Jestes said in her testimony that she could not confirm that the identity thieves used this data to commit identity fraud, the fact that known identity thieves acquired this information increases the possibility that the crime occurred. I based this analysis on the second and third risk factors—who had access to and who viewed the data.

The fourth risk factor considers what actions LabMD has taken to reduce the risk of harm to consumers. Michael Daugherty said LabMD notified the consumers listed on the Day Sheets on March 27, 2013. LabMD mitigated some of the risk of harm for these consumers with notification and tools like credit monitoring. Even though LabMD provided notice, however, there is a strong possibility some of the approximately 600 consumers will still fall victim to identity theft and identity fraud. In particular, the unauthorized disclosure of SSNs creates the opportunity for identity crimes over a long period of time since consumers don't typically change their SSNs after being notified of a breach. Changing an SSN can be a cumbersome process and doesn't necessarily solve all problems. For example, government agencies and private businesses maintain records under consumers' "old" SSNs, and credit reporting companies may use "old" SSNs to identify credit records.[19]

In my experience, unauthorized disclosures of SSNs increases the risk of identity crimes for consumers. Only a small percentage of consumers who receive notification of a breach will call

[19] "Identity Theft and Your Social Security Number," p. 7, by Social Security Administration, December 2013. From http://www.socialsecurity.gov/pubs/EN-05-10064.pdf.

Exhibit 17

into consumer hotlines. An even smaller percentage will take advantage of free credit monitoring. According to Michael Daugherty's March 4, 2014, testimony, approximately 12 percent of the consumers notified enrolled in credit monitoring. Since most consumers won't take any actions to protect themselves—opt in to credit monitoring or set a fraud alert—even after knowing they are at elevated risk of identity crimes, they become even more vulnerable to these crimes.

Use of SSNs in Day Sheets

The FTC analysis of the approximately 600 SSNs using the CLEAR database revealed that 314 SSNs had multiple names listed. I eliminated those that were due to misspellings, name changes, and typos, leaving approximately 100 SSNs that appear to have been used by people with different names. More than one individual using the same SSN is an indicator that identity thieves may have used this information to commit identity theft.

The Sacramento Police Department arrested two known identity thieves who had access to LabMD's sensitive personal information, which increases the risk of harm for the approximately 600 consumers affected by the unauthorized disclosure of their sensitive personal information.

Consumer Harm from Failing to Provide Reasonable and Appropriate Security

Setting aside the unauthorized P2P disclosure and the unauthorized Sacramento disclosure, LabMD's failure to provide reasonable and appropriate security for all its consumers' personal information maintained on its computer networks creates an elevated risk of unauthorized disclosure of this information. This elevated risk, in turn, is likely to cause substantial harm to consumers, in the form of the identity crimes I previously discussed (i.e., identity theft, identity fraud, and medical identity theft). These crimes cause a wide range of economic and non-economic harms to consumers.

Cyber criminals are targeting healthcare organizations because of the high value of sensitive medical information. Organizations with inadequate data security programs are vulnerable to unauthorized disclosures of sensitive personal information. A recently published report by the SANS Institute (an organization that provides security training and certification) found that healthcare systems are the target of cyber thieves, increasing the risk of data theft and fraud.[20]

[20] *SANS Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*, p. 4, by Barbara Filkins, sponsored by Norse, February 2014. From http://norse-corp.com/HealthcareReport2014.html.

Exhibit 17

Submitted by

Rick Kam, President and Co-Founder of ID Experts

Exhibit 17

Appendix A: CV

Rick Kam CV

Date Updated: 1-30-2014

I. **Title:** President and co-founder, ID Experts

II. Work Experience—Present

Rick Kam, Certified Information Privacy Professional (CIPP/US), is president and co-founder of ID Experts, based in Portland, Oregon. He has extensive experience leading organizations in the development of policies and solutions to address the growing problem of protecting protected health information (PHI) and personally identifiable information (PII), and remediating privacy incidents, identity theft, and medical identity theft.

Mr. Kam leads and participates in several cross-industry data privacy groups, speaks at conferences and webinars, and regularly contributes original articles, including a monthly guest article in *Government Health IT*, and offers commentary to privacy, data breach risk, and IT publications. He is often quoted as a resource in news articles about medical identity theft, privacy and data breach.

III. About ID Experts

Co-founded by Kam in 2003, ID Experts delivers services that address the organizational risks associated with sensitive personal data, specifically protected health information (PHI) and personally identifiable information (PII). The teams that Kam has supervised at ID Experts have managed hundreds of data breach incidents, protects millions of individuals, and serves leading healthcare providers, insurance organizations, universities, and government agencies and is exclusively endorsed by the American Hospital Association.

IV. Affiliations and Organizations

As a privacy professional, I actively work on initiatives that focus on data privacy to protect consumers and their sensitive personal information, and I belong to or have belonged to the following organizations:

- Chair of PHI Protection Network (PPN), an interactive network of privacy professionals focused on expediting the adoption of best practices to protect sensitive personal medical information. (2012 - present)

- Chair of The Santa Fe Group Vendor Council ID Management Working Group, which published *Victims' Rights: Fighting Identity Crime on the Front Lines,* February 2009.

Exhibit 17

This white paper explores trends in identity crimes, the victim's experience, and proposes a victim's "bill of rights." (2008- 2012)

- Chair of the American National Standards Institute (ANSI) Identity Management Standards Panel "PHI Project," a seminal research effort to measure financial risk and implications of data breach in healthcare, led by the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with the Shared Assessments Program and the Internet Security Alliance (ISA). The "PHI Project" produced *The Financial Impact of Breached Protected Health Information*. (2011 - 2012)

- Co-Chair of three other cross-industry working groups that published whitepapers on assessing cyber and data breach risks. The reports include *IDSP Workshop Report: Measuring Identity Theft*; *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*; and *The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*. (2007 - 2012)

- Contributor to the Research Planning Committee for the University of Texas Center for Identity, which focuses on identity management and identity theft risk mitigation best practices. ID Experts provided case studies of identity crimes to an analytical repository of identity threats and counter measures called *Identity Threat Assessment and Prediction* (ITAP). (2009 - present)

- Member of the International Association for Privacy Professionals (IAPP), the most comprehensive, member-based privacy community and resource. Mr. Kam maintains a Certified Information Privacy Professional CIPP/US certification for data privacy. (2010 - present)

- Member of Healthcare Information and Management Systems Society (HIMSS), a global, member-based non-profit focused on the betterment of healthcare information technology. (2010 - present)

- Member of Health Care Compliance Association (HCCA), a member-based non-profit that provides training, certification and resources in support of ethics and regulatory compliance in healthcare. (2011-present)

- Founding member of the Medical Identity Fraud Alliance (MIFA), a group of over 40 private and public industry members in the fight against medical identity theft and medical fraud. (2013 - present)

V. **Speaking Engagements**

- HCCA 2014 Compliance Institute, March-April, 2014 (scheduled)

Exhibit 17

Topic: *Evolving Cyber Threats to PHI: How Can We Safeguard Data to Lessen the Frequency and Severity of Data Breaches*

- National HIPAA Summit, February 5-7, 2014
  Topic: *HIPAA Security*

- The National Health Care Anti-Fraud Association (NHCAA) Institute for Health Care Fraud Prevention, 2013 Annual Training Conference, November 2013

  Topic: *Electronic Health Records & Cyber Crime*

- IAPP Practical Privacy Series, October 2013
  Topic: *Vendor and Data Strategy: The CVS Caremark Case Study*

- ID Experts Webinar, September 23, 2013
  Topic: *HIPAA Omnibus Rule Kicks Off*

- Federal Trade Commission Panel, May 2013
  Topic: *Senior Identity Theft: A Problem in This Day and Age*

- HCCA 2013 Compliance Institute, April 2013
  Topic: *Mobile Threats and How Healthcare Can Reduce Risks*

- PHI Protection Network, March 2013
  Topic: *Understanding the Complexities of PHI Privacy and Security: Turning PHI Security Into a Competitive Advantage*

- American Hospital Association Webinar, August, 2012
  Topic: *Data Breach Containment in an Uncontained World: Featuring a Case Study from Henry Ford Hospital*

- ID Experts Webinar, April, 2012
  Topic: *How to Mitigate Risks, Liabilities, & Costs of Data Breach of Health Info by Third Parties*

- PHI Project Webinar, March 2012
  Topic: *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*

- ID Experts Webinar, December, 2011
  Topic: *Second Annual Benchmark Survey on Patient Privacy and Data Security*

Exhibit 17

- ID Experts Webinar, October, 2011
  Topic: *Minimizing Risks of Lawsuits and Fines when Managing a Data Breach Response*

- IAPP Global Privacy Summit, March 2011
  Topic: *Early Preview: Results from ANSI Working Group on Financial Impact of Unauthorized Disclosure of PII & PHI*

- ID Experts Webinar, November, 2010
  Topic: *Ponemon Institute Benchmark Study on Patient Privacy and Data Security*

- ID Experts Webinar, July, 2010
  Topic: *Avoiding Increased Risks and Liabilities Under the Just Released HITECH/HIPAA Rules*

- ID Experts Webinar, May, 2010
  Topic: *Are You Ready for Data Breaches under the New HITECH Act?*

- IAPP Global Privacy Summit, April 2010
  Topic: *Data Breach Risks and the HITECH Act: Best Practices for Risk Assessments, Notification and Compliance*

- Blue Ribbon Panel Discussion, November 2010
  Topic: *HIPAA Security Risk Analysis Do's and Don'ts*

- Blue Ribbon Panel Discussion, August 2010
  Topic: *Chain of Trust: Implications for BAs and Subcontractors*

- HIMSS Analytics Webinar, November 2009
  Topic: *2009 HIMSS Analytics Report: Taking a Pulse on HITECH, Are Hospitals and Associates Ready?*

- Santa Fe Group Panel Discussion Webinar, April 2009
  Topic: *Identity Crime Trends and Victims Bill of Rights*

- Javelin Strategy and Research Webinar, January, 2009
  Topic: *Data Breach Defense 2009: Prevention, Detection and Resolution Strategies to Help Protect Your Bottom Line*

- Association of Certified Fraud Examiners (ACFE), July 2008
  Topic: *Anatomy of a Data Breach Response*

- Federal Office Systems Exposition (FOSE) Conference, April 2008

Exhibit 17

Topic: *Independent Risk Analysis: Providing Public Agencies a More Effective Solution to Mitigate Risk*

- National Association of Independent Fee Appraisers, November 2005
  Topic: *Identity Theft*

- Arizona Bankers Association & Federal Bureau of Investigation, Financial Institutions Fraud & Security Seminar, September 2005
  Topic: *Avoid the Crisis: Reduce the Chance Your Bank and Customers Will Be Hit*

VI. Education

Kam received his BA in Management and Marketing from the University of Hawaii, Honolulu, HI.

VII.Published Works

Key articles Mr. Kam has authored:

- **Medical Identity Theft**

  5 Not-So-Merry Tales of Healthcare Fraud Dark Side
  By Rick Kam and Christine Arevalo, *Government Health IT*, December 20, 2013
  http://www.govhealthit.com/news/5-not-so-merry-tales-healthcare-fraud-dark-side

  The Surprising Truth About Medical ID Thieves
  By Rick Kam, *Government Health IT*, October 11, 2013
  http://www.govhealthit.com/news/surprising-truth-about-medical-id-thieves-EHR-ACA-privacy-security

  The Growing Threat of Medical Identity Fraud: A Call to Action
  By The Medical Identity Fraud Alliance with Rick Kam as Contributor, July 2013
  http://medidfraud.org/the-growing-threat-of-medical-identity-theft-a-call-to-action/

  8 Ways to Fight Medical ID Theft
  By Rick Kam, *Government Health IT,* June 17, 2013
  http://www.govhealthit.com/news/commentary-8-ways-fight-medical-id-theft

  Victim's Rights: Fighting Identity Crime on the Front Lines
  By The Santa Fe Group with Rick Kam as Chair, February 2009

  http://santa-fe-group.com/wp-content/uploads/2010/07/SFG-Identity-Crime-Bill-of-Rights-Feb09.pdf

Exhibit 17

- **Protected Health Information (PHI)**

  What is Your PHI worth?
  By Rick Kam, *Government Health IT*, February 21, 2013
  http://www.govhealthit.com/news/what-your-phi-worth

  The Financial Impact of Breached Protected Health Information
  Rick Kam, contributor. Published by the American National Standards Institute (ANSI), via its Identity Theft Protection and Identity Management Standards Panel (IDSP), in partnership with The Santa Fe Group/Shared Assessments Program Healthcare Working Group, and the Internet Security Alliance (ISA), 2012
  http://webstore.ansi.org/phi/

  PHI Protection Network Announced
  By Rick Kam, ID Experts Blog, October 17, 2012
  http://www2.idexpertscorp.com/blog/single/phi-protection-network-announced/

  The Lifecycle of PHI and Mobile Device Insecurity
  By Rick Kam, *Government Health IT*, June 18, 2012
  http://www.govhealthit.com/news/lifecycle-phi-and-mobile-device-insecurity

  Protected Health Information Should Come with a Disclaimer – "Handle with Care"
  By Rick Kam, ID Experts Blog, March 5, 2012
  http://www2.idexpertscorp.com/blog/single/protected-health-information-should-come-with-a-disclaimer-handle-with-care/

  Protecting PHI: An Industry Initiative and Imperative
  By Rick Kam, ID Experts Blog, April 22, 2011
  http://www2.idexpertscorp.com/blog/single/protecting-phi-an-industry-initiative-and-imperative/

  ANSI and Shared Assessments PHI Project Launched
  By Rick Kam, ID Experts Blog, March 23, 2011
  http://www2.idexpertscorp.com/blog/single/ansi-and-shared-assessments-phi-project-launched/

- **Identity Theft**

  IDSP Workshop Report: Measuring Identity Theft
  Rick Kam, contributor. Published by the American National Standards Institute's (ANSI) Identity Theft Prevention and Identity Management Standards Panel (IDSP), 2009

Exhibit 17

http://webstore.ansi.org/identitytheft/#Measuring

- **Data Breach**

  Data Breaches: 10 Years in Review
  By Rick Kam, ID Experts Blog, July 10, 2013
  http://www2.idexpertscorp.com/blog/single/data-breaches-10-years-in-review/

  2013: The Year of the Data Breach: 11 Data Security Tips to Immunize Your Organization
  By Rick Kam, ID Experts Blog, January 9, 2013
  http://www2.idexpertscorp.com/blog/single/2013-the-year-of-the-data-breach-11-data-security-tips-to-immunize-your-org/

  Why Healthcare Data Breaches Are a C-Suite Concern
  By Rick Kam and Larry Ponemon, *Forbes*, December 7, 2012
  http://www.forbes.com/sites/ciocentral/2012/12/07/why-healthcare-data-breaches-are-a-c-suite-concern/

  5 Key Recommendations to Minimize Data Breaches
  By Rick Kam, *HITECH Answers*, December 6, 2012
  http://www.hitechanswers.net/5-key-recommendations-to-minimize-data-breaches/

  New Ponemon Study Reveals "Common-Cold Frequency" of Data Breaches
  By Rick Kam, ID Experts Blog, December 5, 2012
  http://www2.idexpertscorp.com/blog/single/new-ponemon-study-reveals-common-cold-frequency-of-data-breaches/

  Three Top Data Breach Threats
  By Rick Kam and Jeremy Henley, *Western Pennsylvania Hospital News*, November 1, 2012
  http://www.pageturnpro.com/Western-PA-Hospital-News/41635-Western-PA-Hospital-News,-Issue-10/index.html#22

  Reducing the Risk of a Breach of PHI from Mobile Devices
  By Rick Kam, *HITECH Answers*, September 26, 2012
  http://www.hitechanswers.net/reducing-the-risk-of-a-breach-of-phi-from-mobile-devices/

  Healthcare Data Breaches: Handle with Care
  By Rick Kam and Jeremy Henley, *Property Casualty 360*, March 20, 2012

Exhibit 17

http://www.propertycasualty360.com/2012/03/20/healthcare-data-breaches-handle-with-care

What's Driving the Rise in Data Breaches?
By Rick Kam and Jeremy Henley, *Property Casualty 360*, March 14, 2012
http://www.propertycasualty360.com/2012/03/14/whats-driving-the-rise-in-data-breaches

Wi-Fi Networks Leaving Patients Susceptible to Loss of Personal Data
By Rick Kam, ID Experts Blog, July 20, 2011
http://www2.idexpertscorp.com/blog/single/wi-fi-networks-leaving-patients-susceptible-to-loss-of-personal-data/

- **Privacy**

  Google Glass and Other Devices Presenting New Crop of Privacy Risks
  By Rick Kam, *Government Health IT*, August 14, 2013
  http://www.govhealthit.com/news/google-glass-and-other-devices-presenting-new-crop-privacy-risks

  5 Steps to Protect Patient Privacy
  By Rick Kam and Larry Ponemon, *Government Health IT*, December 07, 2012
  http://www.govhealthit.com/news/5-steps-protect-patient-privacy

  Electronic Health Records vs. Patient Privacy: Who Will Win?
  By Rick Kam and Doug Pollack, *IAPP*, October 23, 2012
  https://www.privacyassociation.org/publications/2012_11_01_the_healthcare_privacy_balance

  Is Privacy a Constitutional Right in America?
  By Rick Kam, ID Experts Blog, May 27, 2011
  http://www2.idexpertscorp.com/blog/single/is-privacy-a-constitutional-right-in-america/

- **Cyber Risk/Security**

  4 Steps for Business Associates to Comply with Omnibus HIPAA
  By Rick Kam and Mahmood Sher-Jan, *Government Health IT*, September 20, 2013
  http://www.govhealthit.com/news/4-steps-business-associates-comply-omnibus-hipaa

  3 Ways to Make Data Protection More Patient-Centric
  By Rick Kam, *Government Health IT*, April 9, 2013
  http://www.govhealthit.com/news/3-steps-building-patient-centric-privacy-and-security

Exhibit 17

The Financial Management of Cyber Risk: An Implementation Framework for CFOs
Rick Kam, contributor. Published by the American National Standards Institute (ANSI)/ Internet Security Alliance (ISA), 2010
http://webstore.ansi.org/cybersecurity.aspx

The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask
Rick Kam, contributor. Published by the American National Standards Institute (ANSI)/ Internet Security Alliance (ISA), 2008

http://www.ansi.org/meetings_events/events/cyber_risk09.aspx?menuid=8

- **Regulatory/Compliance**

  Privacy and Security Compliance Wish List 2014
  By Rick Kam, *Government Health IT,* January 14, 2014
  http://www.govhealthit.com/blog/privacy-and-security-pros-compliance-wish-list-2014

  11 Data Security Tips for a Healthy Organization in 2013
  By Rick Kam, *Government Health IT*, January 08, 2013
  http://www.govhealthit.com/news/11-data-security-tips-healthy-organization-2013

Appendix B: Literature Review

Date	Publication/Title	URL	Author	Description
Feb. 2014	2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends	https://www.javelinstrategy.com/brochure/314	Javelin Strategy & Research	Analysis of fraud trends to help consumers, financial institutions, and businesses prevent, detect, and resolve fraud.
Feb. 2014	SANS Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon	http://norse-corp.com/HealthcareReport2014.html	Barbara Filkins, sponsored by Norse	Discusses the vulnerabilities of the healthcare industry to cyberthreats.
Dec. 2013	Identity Theft and Your Social Security Number	http://www.socialsecurity.gov/pubs/EN-05-10064.pdf	Social Security Administration	Consumer tips on protecting against SSN-related identity theft.

Exhibit 17

Dec. 2013	Victims of Identity Theft, 2012	http://www.bjs.gov/content/pub/pdf/vit12.pdf	Bureau of Justice Statistics, U.S. Department of Justice	In-depth statistical analysis on identity theft victims in 2012.
Nov. 7, 2013	TIGTA Report: The IRS Needs to Improve Customer Service for Identity Theft Victims	http://www.treasury.gov/tigta/press/press_tigta-2013-40.htm	Treasury Inspector General for Tax Administration	Press release
Oct. 2013	First Aid for Medical Identity Theft: Tips for Consumers	https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft.pdf	Calif. Dept. of Justice	Consumer information on medical identity theft.
Oct. 2013	Medical Identity Theft: Recommendations for the Age of Electronic Medical Records	https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf	Kamala D. Harris, Attorney General, Calif. Dept. of Justice	Recommendations to help prevent, detect, and mitigate the effects of medical identity theft.
Sept. 20, 2013	Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds	http://www.treasury.gov/tigta/auditreports/2013reports/201340122fr.html	Treasury Inspector General for Tax Administration	Report to determine whether the IRS has improved its programs and procedures to identify and prevent fraudulent tax refunds resulting from identity theft.
Sept. 2013	2013 Survey on Medical Identity Theft	http://medidfraud.org/2013-survey-on-medical-identity-theft/	Ponemon Institute	Measures the prevalence, extent, and impact of medical identity theft in the United States to consumers and the healthcare industry.
April 2013	2013 Data Breach Investigations Report	http://www.verizonenterprise.com/DBIR/2013/	Verizon	Provides global insights into the nature of data breaches that help organizations better understand the threat and take the necessary steps to protect themselves.
January 2013	Tips for Taxpayers, Victims about Identity Theft and Tax Returns	http://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers,-Victims-about-Identity-Theft-and-Tax-Returns	Internal Revenue Service	Consumer tips for protecting against and remediating tax-related identity theft.

Exhibit 17

2013	2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters	https://www.javelinstrategy.com/brochure/276	Javelin Strategy and Research	Analyzes fraud trends in the context of a changing technological and regulatory environment in order to inform consumers, financial institutions, and businesses on the most effective means of fraud prevention, detection, and resolution.
2013	Cybercrime and the Healthcare Industry	http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf	RSA, The Security Division of EMC	Discusses the growing threat of cybercrime to electronic healthcare data.
June 2012	Creating a Trusted Environment: Reducing the Threat of Medical Identity Theft	https://www.himss.org/files/HIMSSorg/content/files/CreatingaTrustedEnvironment_Reducing_the_Threat_of_Medical_Identify_TheftFINAL.pdf	HIMSS Privacy and Security Task Force, Kroll-sponsored	Evaluates risk and mitigation strategies for protecting PHI.
March 2012	The Financial Impact of Breached PHI	http://webstore.ansi.org/phi/	Workgroups	ANSI whitepaper on the financial impact of breached protected health information.
Oct. 2009	IDSP Workshop Report: Measuring Identity Theft	http://webstore.ansi.org/identitytheft/#Measuring	Workgroup #2 of IDSP	Addresses how research companies measure identity crime. Includes a catalog of 166 research projects to date.
Jan. 2009	Medical Identity Theft Final Report	http://www.healthit.gov/sites/default/files/medidtheftreport011509_0.pdf	Booz Allen Hamilton	Recommendations for addressing issues from a “town hall” meeting. Prepared for HHS, and ONC for Health Information Technology.
Nov. 7, 2008	Express Scripts Data Breach Leads to Extortion Attempt	http://blogs.wsj.com/health/2008/11/07/express-scripts-data-breach-leads-to-extortion-attempt/	Sarah Rubenstein, *Wall Street Journal* Health Blog	Article describing two extortion attempts involving patient information.

Exhibit 17

Oct. 2008	Medical Identity Theft Environmental Scan	http://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf	Booz Allen Hamilton	Information and insights about medical Identity theft. Prepared for HHS, and ONC for Health Information Technology.
Sept. 2008	The President's Identity Theft Task Force Report	http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf	Identity Theft Task Force	Documents the Task Force's efforts to implement recommendations for fighting identity theft.
October 2007	Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement	http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf	Center for Identity Management and Information Protection, Utica College	Provides empirical evidence on which law enforcement can base enhanced proactive identity theft control and prevention efforts.
May 2006	Medical Identity Theft: The Information Crime that Can Kill You	http://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/	Pam Dixon	Report on impact of medical identity theft including cases.
July 2005	Identity Theft Literature Review	https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf	Newman and McNally	Identity theft literature review funded by the Department of Justice.
Ongoing	The Facts about MIB	http://www.mib.com/facts_about_mib.html	Medical Information Bureau	Website describing MIB's purpose—enabling companies to offer affordable life and health insurance to customers.

Exhibit 17

Appendix C: State Breach Notification Laws in Effect before May 2008

The number of the Breach Notification Laws in effect before May 2008 is 41. The following list includes the effective dates for each state or territory:

In 2003:

- California (July 1)

In 2005 (12):

- Georgia (May 5)
- North Dakota (June 1)
- Delaware (June 28)
- Florida (July 1)
- Tennessee (July 1)
- Washington (July 24)
- Texas (September 1)
- Arkansas (August 12)
- Virgin Islands (October 17)
- North Carolina (December 1)
- Puerto Rico (December 4)
- New York (December 7)

In 2006 (17):

- Connecticut (January 1)
- Louisiana (January 1)
- Minnesota (January 1)
- Nevada (January 1)
- New Jersey (January 1)
- Maine (January 31)
- Ohio (February 17)
- Montana (March 1)
- Rhode Island (March 1)
- Wisconsin (March 31)
- Pennsylvania (June 20)
- Illinois (June 27)
- Idaho (July 1)
- Indiana (July 1)
- Nebraska (July 14)
- Colorado (September 1)
- Arizona (December 31)

In 2007 (10):

Exhibit 17

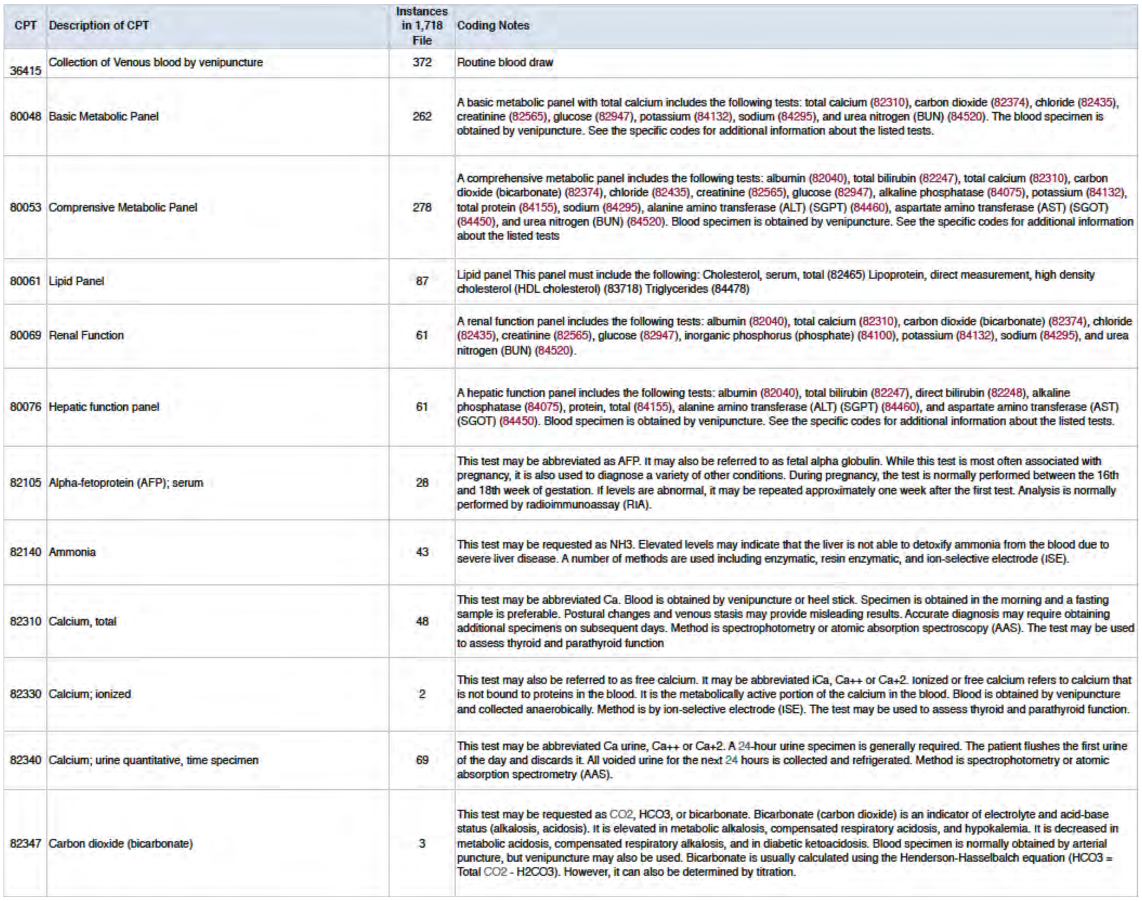
- Hawaii (January 1)
- Kansas (January 1)
- New Hampshire (January 1)
- Utah (January 1)
- Vermont (January 1)
- District of Columbia (July 1)
- Wyoming (July 1)
- Michigan (July 2)
- Oregon (October 1)
- Massachusetts (October 31)

In 2008:

- Maryland (January 1)

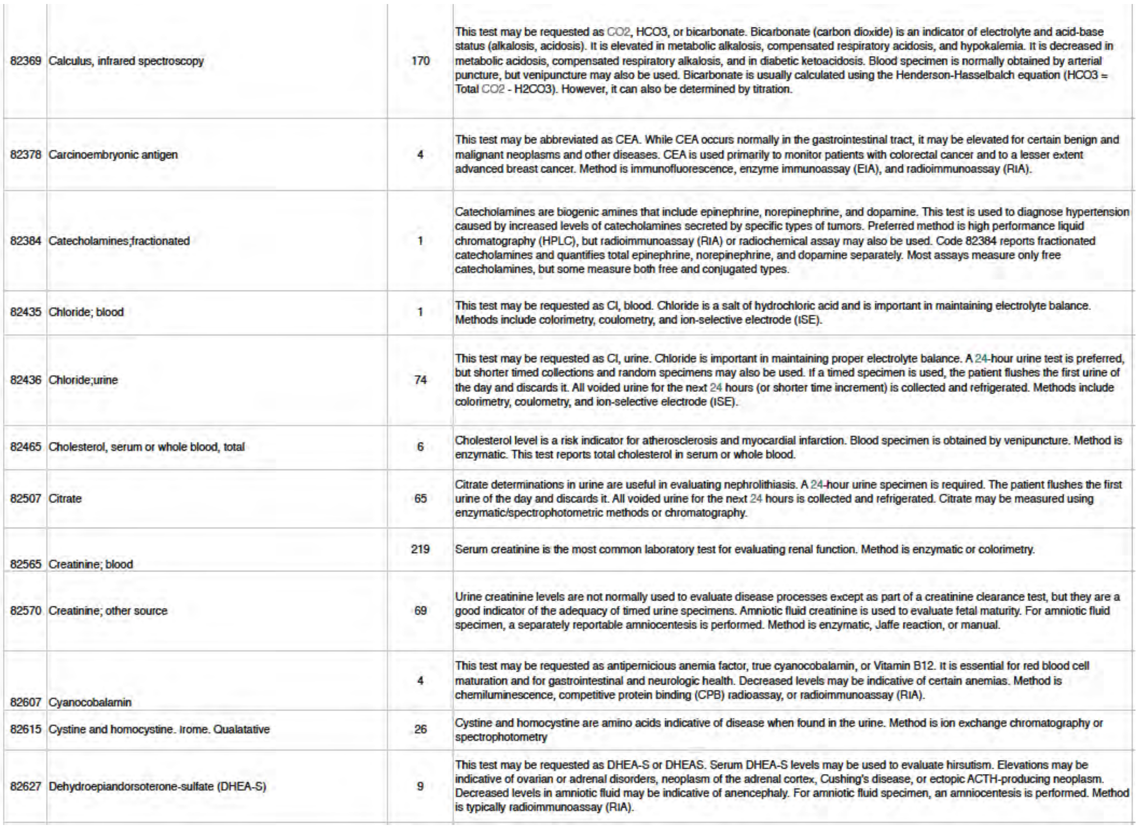
Exhibit 17

Appendix D: List of CPT Codes



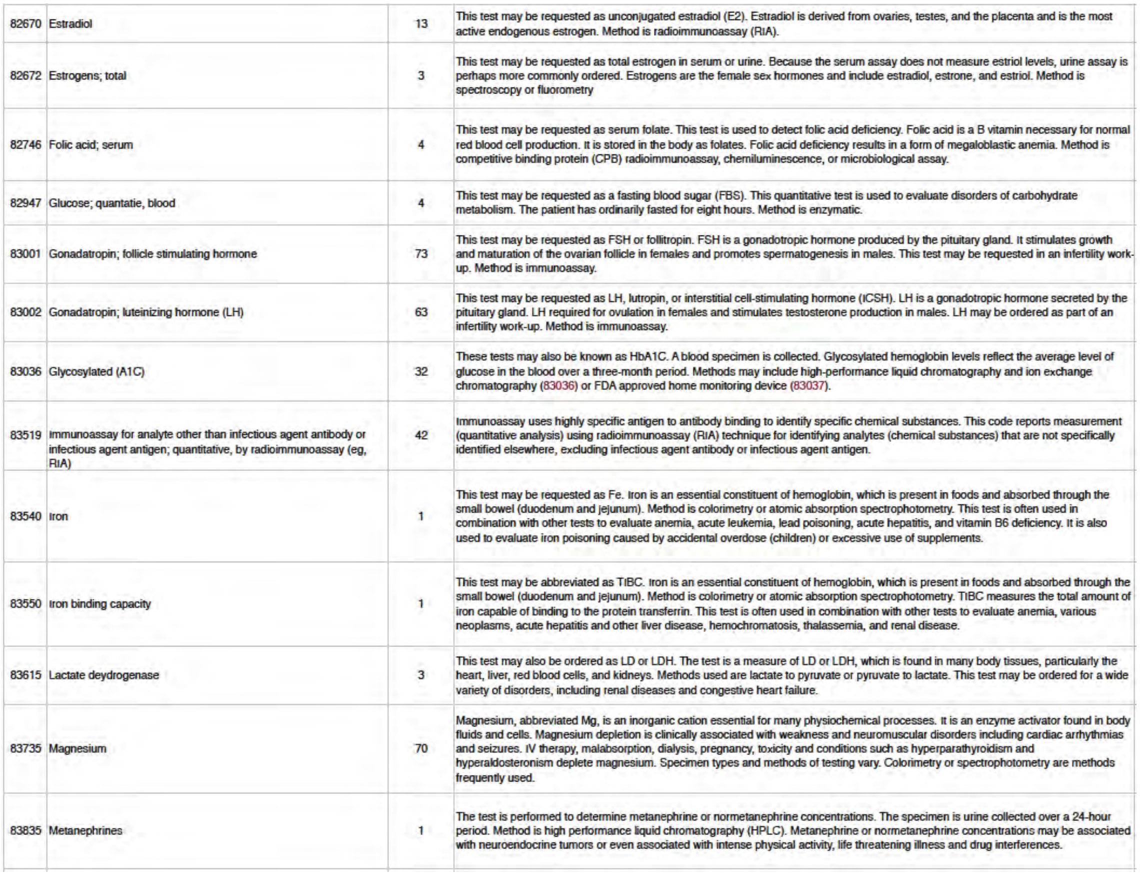
CPT	Description of CPT	Instances in 1,718 File	Coding Notes
36415	Collection of Venous blood by venipuncture	372	Routine blood draw
80048	Basic Metabolic Panel	262	A basic metabolic panel with total calcium includes the following tests: total calcium (82310), carbon dioxide (82374), chloride (82435), creatinine (82565), glucose (82947), potassium (84132), sodium (84295), and urea nitrogen (BUN) (84520). The blood specimen is obtained by venipuncture. See the specific codes for additional information about the listed tests.
80053	Comprensive Metabolic Panel	278	A comprehensive metabolic panel includes the following tests: albumin (82040), total bilirubin (82247), total calcium (82310), carbon dioxide (bicarbonate) (82374), chloride (82435), creatinine (82565), glucose (82947), alkaline phosphatase (84075), potassium (84132), total protein (84155), sodium (84295), alanine amino transferase (ALT) (SGPT) (84460), aspartate amino transferase (AST) (SGOT) (84450), and urea nitrogen (BUN) (84520). Blood specimen is obtained by venipuncture. See the specific codes for additional information about the listed tests
80061	Lipid Panel	87	Lipid panel This panel must include the following: Cholesterol, serum, total (82465) Lipoprotein, direct measurement, high density cholesterol (HDL cholesterol) (83718) Triglycerides (84478)
80069	Renal Function	61	A renal function panel includes the following tests: albumin (82040), total calcium (82310), carbon dioxide (bicarbonate) (82374), chloride (82435), creatinine (82565), glucose (82947), inorganic phosphorus (phosphate) (84100), potassium (84132), sodium (84295), and urea nitrogen (BUN) (84520).
80076	Hepatic function panel	61	A hepatic function panel includes the following tests: albumin (82040), total bilirubin (82247), direct bilirubin (82248), alkaline phosphatase (84075), protein, total (84155), alanine amino transferase (ALT) (SGPT) (84460), and aspartate amino transferase (AST) (SGOT) (84450). Blood specimen is obtained by venipuncture. See the specific codes for additional information about the listed tests.
82105	Alpha-fetoprotein (AFP); serum	28	This test may be abbreviated as AFP. It may also be referred to as fetal alpha globulin. While this test is most often associated with pregnancy, it is also used to diagnose a variety of other conditions. During pregnancy, the test is normally performed between the 16th and 18th week of gestation. If levels are abnormal, it may be repeated approximately one week after the first test. Analysis is normally performed by radioimmunoassay (RIA).
82140	Ammonia	43	This test may be requested as NH3. Elevated levels may indicate that the liver is not able to detoxify ammonia from the blood due to severe liver disease. A number of methods are used including enzymatic, resin enzymatic, and ion-selective electrode (ISE).
82310	Calcium, total	48	This test may be abbreviated Ca. Blood is obtained by venipuncture or heel stick. Specimen is obtained in the morning and a fasting sample is preferable. Postural changes and venous stasis may provide misleading results. Accurate diagnosis may require obtaining additional specimens on subsequent days. Method is spectrophotometry or atomic absorption spectroscopy (AAS). The test may be used to assess thyroid and parathyroid function
82330	Calcium; ionized	2	This test may also be referred to as free calcium. It may be abbreviated iCa, Ca++ or Ca+2. Ionized or free calcium refers to calcium that is not bound to proteins in the blood. It is the metabolically active portion of the calcium in the blood. Blood is obtained by venipuncture and collected anaerobically. Method is by ion-selective electrode (ISE). The test may be used to assess thyroid and parathyroid function.
82340	Calcium; urine quantitative, time specimen	69	This test may be abbreviated Ca urine, Ca++ or Ca+2. A 24-hour urine specimen is generally required. The patient flushes the first urine of the day and discards it. All voided urine for the next 24 hours is collected and refrigerated. Method is spectrophotometry or atomic absorption spectrometry (AAS).
82347	Carbon dioxide (bicarbonate)	3	This test may be requested as CO2, HCO3, or bicarbonate. Bicarbonate (carbon dioxide) is an indicator of electrolyte and acid-base status (alkalosis, acidosis). It is elevated in metabolic alkalosis, compensated respiratory acidosis, and hypokalemia. It is decreased in metabolic acidosis, compensated respiratory alkalosis, and in diabetic ketoacidosis. Blood specimen is normally obtained by arterial puncture, but venipuncture may also be used. Bicarbonate is usually calculated using the Henderson-Hasselbalch equation (HCO3 = Total CO2 - H2CO3). However, it can also be determined by titration.

Exhibit 17



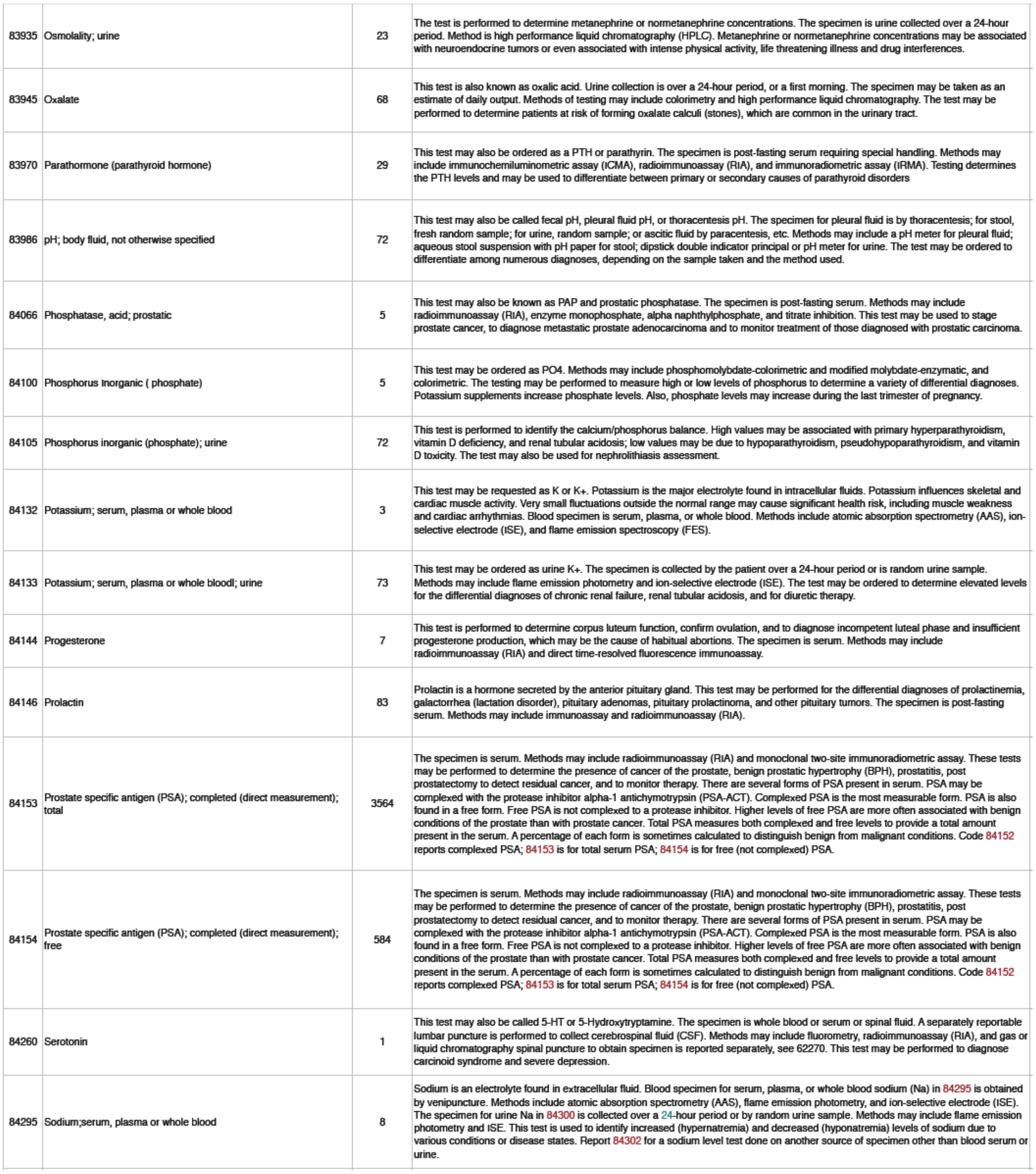
82369	Calculus, infrared spectroscopy	170	This test may be requested as CO2, HCO3, or bicarbonate. Bicarbonate (carbon dioxide) is an indicator of electrolyte and acid-base status (alkalosis, acidosis). It is elevated in metabolic alkalosis, compensated respiratory acidosis, and hypokalemia. It is decreased in metabolic acidosis, compensated respiratory alkalosis, and in diabetic ketoacidosis. Blood specimen is normally obtained by arterial puncture, but venipuncture may also be used. Bicarbonate is usually calculated using the Henderson-Hasselbalch equation (HCO3 = Total CO2 - H2CO3). However, it can also be determined by titration.
82378	Carcinoembryonic antigen	4	This test may be abbreviated as CEA. While CEA occurs normally in the gastrointestinal tract, it may be elevated for certain benign and malignant neoplasms and other diseases. CEA is used primarily to monitor patients with colorectal cancer and to a lesser extent advanced breast cancer. Method is immunofluorescence, enzyme immunoassay (EIA), and radioimmunoassay (RIA).
82384	Catecholamines;fractionated	1	Catecholamines are biogenic amines that include epinephrine, norepinephrine, and dopamine. This test is used to diagnose hypertension caused by increased levels of catecholamines secreted by specific types of tumors. Preferred method is high performance liquid chromatography (HPLC), but radioimmunoassay (RIA) or radiochemical assay may also be used. Code 82384 reports fractionated catecholamines and quantifies total epinephrine, norepinephrine, and dopamine separately. Most assays measure only free catecholamines, but some measure both free and conjugated types.
82435	Chloride; blood	1	This test may be requested as Cl, blood. Chloride is a salt of hydrochloric acid and is important in maintaining electrolyte balance. Methods include colorimetry, coulometry, and ion-selective electrode (ISE).
82436	Chloride;urine	74	This test may be requested as Cl, urine. Chloride is important in maintaining proper electrolyte balance. A 24-hour urine test is preferred, but shorter timed collections and random specimens may also be used. If a timed specimen is used, the patient flushes the first urine of the day and discards it. All voided urine for the next 24 hours (or shorter time increment) is collected and refrigerated. Methods include colorimetry, coulometry, and ion-selective electrode (ISE).
82465	Cholesterol, serum or whole blood, total	6	Cholesterol level is a risk indicator for atherosclerosis and myocardial infarction. Blood specimen is obtained by venipuncture. Method is enzymatic. This test reports total cholesterol in serum or whole blood.
82507	Citrate	65	Citrate determinations in urine are useful in evaluating nephrolithiasis. A 24-hour urine specimen is required. The patient flushes the first urine of the day and discards it. All voided urine for the next 24 hours is collected and refrigerated. Citrate may be measured using enzymatic/spectrophotometric methods or chromatography.
82565	Creatinine; blood	219	Serum creatinine is the most common laboratory test for evaluating renal function. Method is enzymatic or colorimetry.
82570	Creatinine; other source	69	Urine creatinine levels are not normally used to evaluate disease processes except as part of a creatinine clearance test, but they are a good indicator of the adequacy of timed urine specimens. Amniotic fluid creatinine is used to evaluate fetal maturity. For amniotic fluid specimen, a separately reportable amniocentesis is performed. Method is enzymatic, Jaffe reaction, or manual.
82607	Cyanocobalamin	4	This test may be requested as antipernicious anemia factor, true cyanocobalamin, or Vitamin B12. It is essential for red blood cell maturation and for gastrointestinal and neurologic health. Decreased levels may be indicative of certain anemias. Method is chemiluminescence, competitive protein binding (CPB) radioassay, or radioimmunoassay (RIA).
82615	Cystine and homocystine. Irome. Qualatative	26	Cystine and homocystine are amino acids indicative of disease when found in the urine. Method is ion exchange chromatography or spectrophotometry
82627	Dehydroepiandorsoterone-sulfate (DHEA-S)	9	This test may be requested as DHEA-S or DHEAS. Serum DHEA-S levels may be used to evaluate hirsutism. Elevations may be indicative of ovarian or adrenal disorders, neoplasm of the adrenal cortex, Cushing's disease, or ectopic ACTH-producing neoplasm. Decreased levels in amniotic fluid may be indicative of anencephaly. For amniotic fluid specimen, an amniocentesis is performed. Method is typically radioimmunoassay (RIA).

Exhibit 17



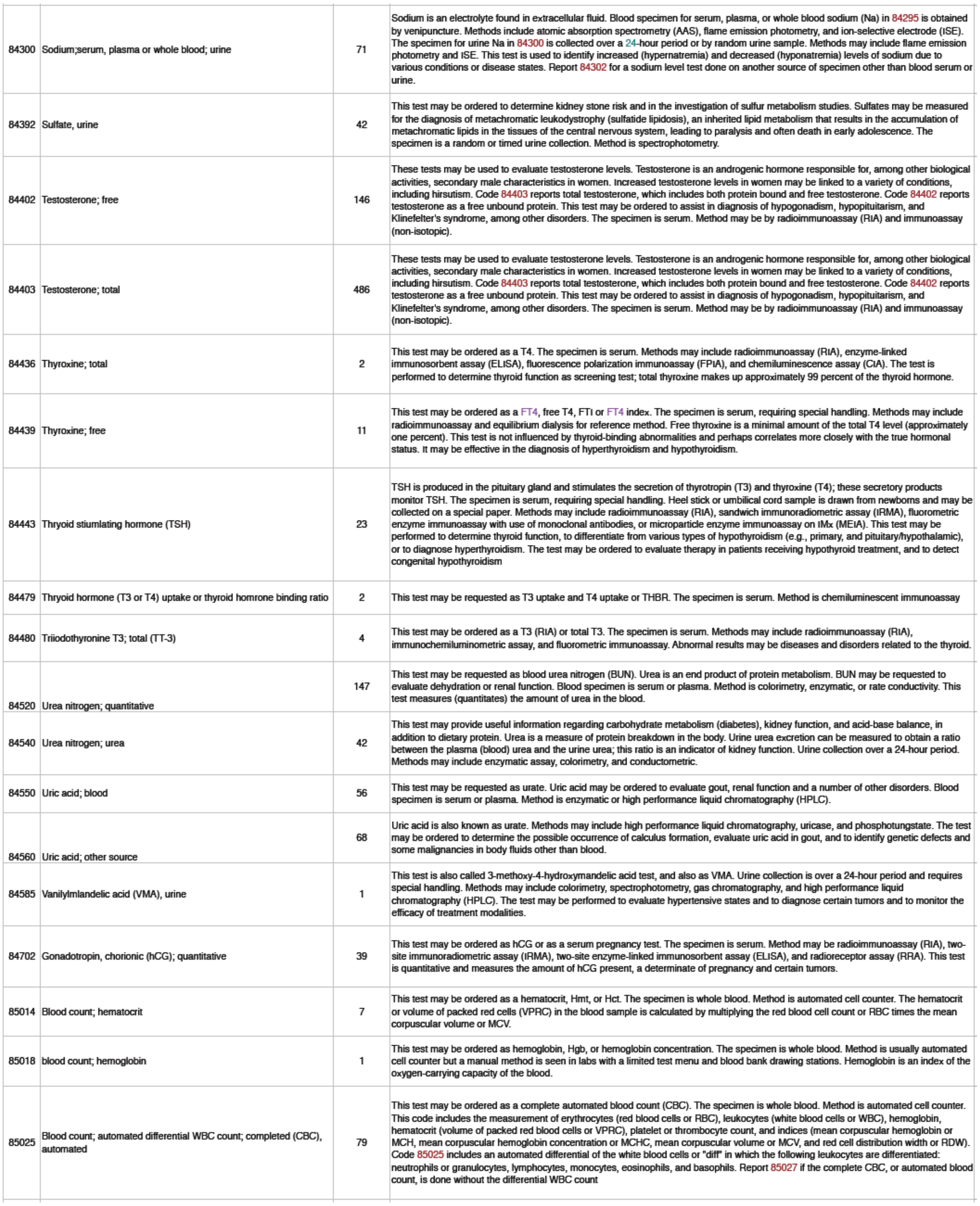
82670	Estradiol	13	This test may be requested as unconjugated estradiol (E2). Estradiol is derived from ovaries, testes, and the placenta and is the most active endogenous estrogen. Method is radioimmunoassay (RIA).
82672	Estrogens; total	3	This test may be requested as total estrogen in serum or urine. Because the serum assay does not measure estriol levels, urine assay is perhaps more commonly ordered. Estrogens are the female sex hormones and include estradiol, estrone, and estriol. Method is spectroscopy or fluorometry
82746	Folic acid; serum	4	This test may be requested as serum folate. This test is used to detect folic acid deficiency. Folic acid is a B vitamin necessary for normal red blood cell production. It is stored in the body as folates. Folic acid deficiency results in a form of megaloblastic anemia. Method is competitive binding protein (CPB) radioimmunoassay, chemiluminescence, or microbiological assay.
82947	Glucose; quantatie, blood	4	This test may be requested as a fasting blood sugar (FBS). This quantitative test is used to evaluate disorders of carbohydrate metabolism. The patient has ordinarily fasted for eight hours. Method is enzymatic.
83001	Gonadatropin; follicle stimulating hormone	73	This test may be requested as FSH or follitropin. FSH is a gonadotropic hormone produced by the pituitary gland. It stimulates growth and maturation of the ovarian follicle in females and promotes spermatogenesis in males. This test may be requested in an infertility work-up. Method is immunoassay.
83002	Gonadatropin; luteinizing hormone (LH)	63	This test may be requested as LH, lutropin, or interstitial cell-stimulating hormone (ICSH). LH is a gonadotropic hormone secreted by the pituitary gland. LH required for ovulation in females and stimulates testosterone production in males. LH may be ordered as part of an infertility work-up. Method is immunoassay.
83036	Glycosylated (A1C)	32	These tests may also be known as HbA1C. A blood specimen is collected. Glycosylated hemoglobin levels reflect the average level of glucose in the blood over a three-month period. Methods may include high-performance liquid chromatography and ion exchange chromatography (83036) or FDA approved home monitoring device (83037).
83519	Immunoassay for analyte other than infectious agent antibody or infectious agent antigen; quantitative, by radioimmunoassay (eg, RIA)	42	Immunoassay uses highly specific antigen to antibody binding to identify specific chemical substances. This code reports measurement (quantitative analysis) using radioimmunoassay (RIA) technique for identifying analytes (chemical substances) that are not specifically identified elsewhere, excluding infectious agent antibody or infectious agent antigen.
83540	Iron	1	This test may be requested as Fe. Iron is an essential constituent of hemoglobin, which is present in foods and absorbed through the small bowel (duodenum and jejunum). Method is colorimetry or atomic absorption spectrophotometry. This test is often used in combination with other tests to evaluate anemia, acute leukemia, lead poisoning, acute hepatitis, and vitamin B6 deficiency. It is also used to evaluate iron poisoning caused by accidental overdose (children) or excessive use of supplements.
83550	Iron binding capacity	1	This test may be abbreviated as TIBC. Iron is an essential constituent of hemoglobin, which is present in foods and absorbed through the small bowel (duodenum and jejunum). Method is colorimetry or atomic absorption spectrophotometry. TIBC measures the total amount of iron capable of binding to the protein transferrin. This test is often used in combination with other tests to evaluate anemia, various neoplasms, acute hepatitis and other liver disease, hemochromatosis, thalassemia, and renal disease.
83615	Lactate deydrogenase	3	This test may also be ordered as LD or LDH. The test is a measure of LD or LDH, which is found in many body tissues, particularly the heart, liver, red blood cells, and kidneys. Methods used are lactate to pyruvate or pyruvate to lactate. This test may be ordered for a wide variety of disorders, including renal diseases and congestive heart failure.
83735	Magnesium	70	Magnesium, abbreviated Mg, is an inorganic cation essential for many physiochemical processes. It is an enzyme activator found in body fluids and cells. Magnesium depletion is clinically associated with weakness and neuromuscular disorders including cardiac arrhythmias and seizures. IV therapy, malabsorption, dialysis, pregnancy, toxicity and conditions such as hyperparathyroidism and hyperaldosteronism deplete magnesium. Specimen types and methods of testing vary. Colorimetry or spectrophotometry are methods frequently used.
83835	Metanephrines	1	The test is performed to determine metanephrine or normetanephrine concentrations. The specimen is urine collected over a 24-hour period. Method is high performance liquid chromatography (HPLC). Metanephrine or normetanephrine concentrations may be associated with neuroendocrine tumors or even associated with intense physical activity, life threatening illness and drug interferences.

Exhibit 17



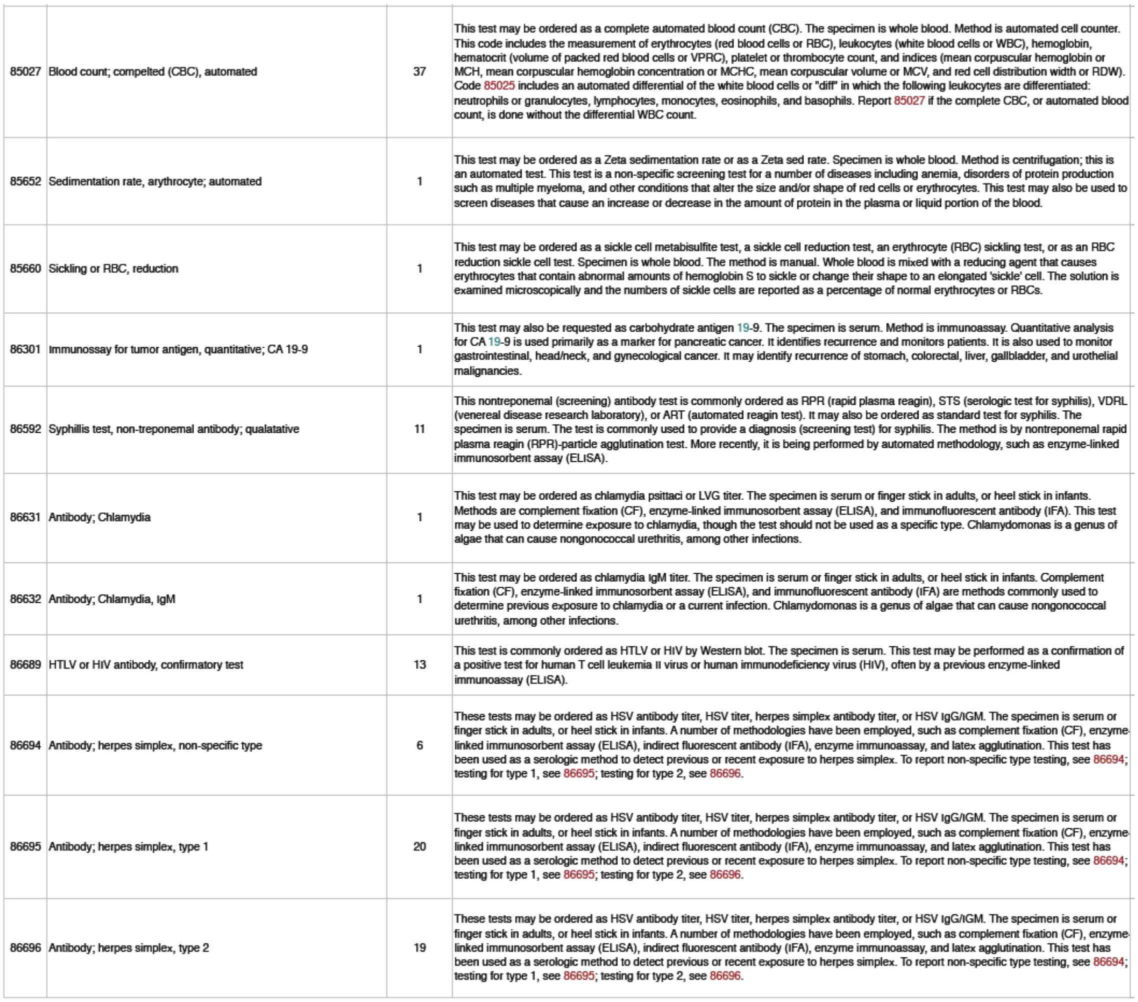
83935	Osmolality; urine	23	The test is performed to determine metanephrine or normetanephrine concentrations. The specimen is urine collected over a 24-hour period. Method is high performance liquid chromatography (HPLC). Metanephrine or normetanephrine concentrations may be associated with neuroendocrine tumors or even associated with intense physical activity, life threatening illness and drug interferences.
83945	Oxalate	68	This test is also known as oxalic acid. Urine collection is over a 24-hour period, or a first morning. The specimen may be taken as an estimate of daily output. Methods of testing may include colorimetry and high performance liquid chromatography. The test may be performed to determine patients at risk of forming oxalate calculi (stones), which are common in the urinary tract.
83970	Parathormone (parathyroid hormone)	29	This test may also be ordered as a PTH or parathyrin. The specimen is post-fasting serum requiring special handling. Methods may include immunochemiluminometric assay (ICMA), radioimmunoassay (RIA), and immunoradiometric assay (IRMA). Testing determines the PTH levels and may be used to differentiate between primary or secondary causes of parathyroid disorders
83986	pH; body fluid, not otherwise specified	72	This test may also be called fecal pH, pleural fluid pH, or thoracentesis pH. The specimen for pleural fluid is by thoracentesis; for stool, fresh random sample; for urine, random sample; or ascitic fluid by paracentesis, etc. Methods may include a pH meter for pleural fluid; aqueous stool suspension with pH paper for stool; dipstick double indicator principal or pH meter for urine. The test may be ordered to differentiate among numerous diagnoses, depending on the sample taken and the method used.
84066	Phosphatase, acid; prostatic	5	This test may also be known as PAP and prostatic phosphatase. The specimen is post-fasting serum. Methods may include radioimmunoassay (RIA), enzyme monophosphate, alpha naphthylphosphate, and titrate inhibition. This test may be used to stage prostate cancer, to diagnose metastatic prostate adenocarcinoma and to monitor treatment of those diagnosed with prostatic carcinoma.
84100	Phosphorus Inorganic (phosphate)	5	This test may be ordered as PO4. Methods may include phosphomolybdate-colorimetric and modified molybdate-enzymatic, and colorimetric. The testing may be performed to measure high or low levels of phosphorus to determine a variety of differential diagnoses. Potassium supplements increase phosphate levels. Also, phosphate levels may increase during the last trimester of pregnancy.
84105	Phosphorus inorganic (phosphate); urine	72	This test is performed to identify the calcium/phosphorus balance. High values may be associated with primary hyperparathyroidism, vitamin D deficiency, and renal tubular acidosis; low values may be due to hypoparathyroidism, pseudohypoparathyroidism, and vitamin D toxicity. The test may also be used for nephrolithiasis assessment.
84132	Potassium; serum, plasma or whole blood	3	This test may be requested as K or K+. Potassium is the major electrolyte found in intracellular fluids. Potassium influences skeletal and cardiac muscle activity. Very small fluctuations outside the normal range may cause significant health risk, including muscle weakness and cardiac arrhythmias. Blood specimen is serum, plasma, or whole blood. Methods include atomic absorption spectrometry (AAS), ion-selective electrode (ISE), and flame emission spectroscopy (FES).
84133	Potassium; serum, plasma or whole bloodl; urine	73	This test may be ordered as urine K+. The specimen is collected by the patient over a 24-hour period or is random urine sample. Methods may include flame emission photometry and ion-selective electrode (ISE). The test may be ordered to determine elevated levels for the differential diagnoses of chronic renal failure, renal tubular acidosis, and for diuretic therapy.
84144	Progesterone	7	This test is performed to determine corpus luteum function, confirm ovulation, and to diagnose incompetent luteal phase and insufficient progesterone production, which may be the cause of habitual abortions. The specimen is serum. Methods may include radioimmunoassay (RIA) and direct time-resolved fluorescence immunoassay.
84146	Prolactin	83	Prolactin is a hormone secreted by the anterior pituitary gland. This test may be performed for the differential diagnoses of prolactinemia, galactorrhea (lactation disorder), pituitary adenomas, pituitary prolactinoma, and other pituitary tumors. The specimen is post-fasting serum. Methods may include immunoassay and radioimmunoassay (RIA).
84153	Prostate specific antigen (PSA); completed (direct measurement); total	3564	The specimen is serum. Methods may include radioimmunoassay (RIA) and monoclonal two-site immunoradiometric assay. These tests may be performed to determine the presence of cancer of the prostate, benign prostatic hypertrophy (BPH), prostatitis, post prostatectomy to detect residual cancer, and to monitor therapy. There are several forms of PSA present in serum. PSA may be complexed with the protease inhibitor alpha-1 antichymotrypsin (PSA-ACT). Complexed PSA is the most measurable form. PSA is also found in a free form. Free PSA is not complexed to a protease inhibitor. Higher levels of free PSA are more often associated with benign conditions of the prostate than with prostate cancer. Total PSA measures both complexed and free levels to provide a total amount present in the serum. A percentage of each form is sometimes calculated to distinguish benign from malignant conditions. Code 84152 reports complexed PSA; 84153 is for total serum PSA; 84154 is for free (not complexed) PSA.
84154	Prostate specific antigen (PSA); completed (direct measurement); free	584	The specimen is serum. Methods may include radioimmunoassay (RIA) and monoclonal two-site immunoradiometric assay. These tests may be performed to determine the presence of cancer of the prostate, benign prostatic hypertrophy (BPH), prostatitis, post prostatectomy to detect residual cancer, and to monitor therapy. There are several forms of PSA present in serum. PSA may be complexed with the protease inhibitor alpha-1 antichymotrypsin (PSA-ACT). Complexed PSA is the most measurable form. PSA is also found in a free form. Free PSA is not complexed to a protease inhibitor. Higher levels of free PSA are more often associated with benign conditions of the prostate than with prostate cancer. Total PSA measures both complexed and free levels to provide a total amount present in the serum. A percentage of each form is sometimes calculated to distinguish benign from malignant conditions. Code 84152 reports complexed PSA; 84153 is for total serum PSA; 84154 is for free (not complexed) PSA.
84260	Serotonin	1	This test may also be called 5-HT or 5-Hydroxytryptamine. The specimen is whole blood or serum or spinal fluid. A separately reportable lumbar puncture is performed to collect cerebrospinal fluid (CSF). Methods may include fluorometry, radioimmunoassay (RIA), and gas or liquid chromatography spinal puncture to obtain specimen is reported separately, see 62270. This test may be performed to diagnose carcinoid syndrome and severe depression.
84295	Sodium;serum, plasma or whole blood	8	Sodium is an electrolyte found in extracellular fluid. Blood specimen for serum, plasma, or whole blood sodium (Na) in 84295 is obtained by venipuncture. Methods include atomic absorption spectrometry (AAS), flame emission photometry, and ion-selective electrode (ISE). The specimen for urine Na in 84300 is collected over a 24-hour period or by random urine sample. Methods may include flame emission photometry and ISE. This test is used to identify increased (hypernatremia) and decreased (hyponatremia) levels of sodium due to various conditions or disease states. Report 84302 for a sodium level test done on another source of specimen other than blood serum or urine.

Exhibit 17



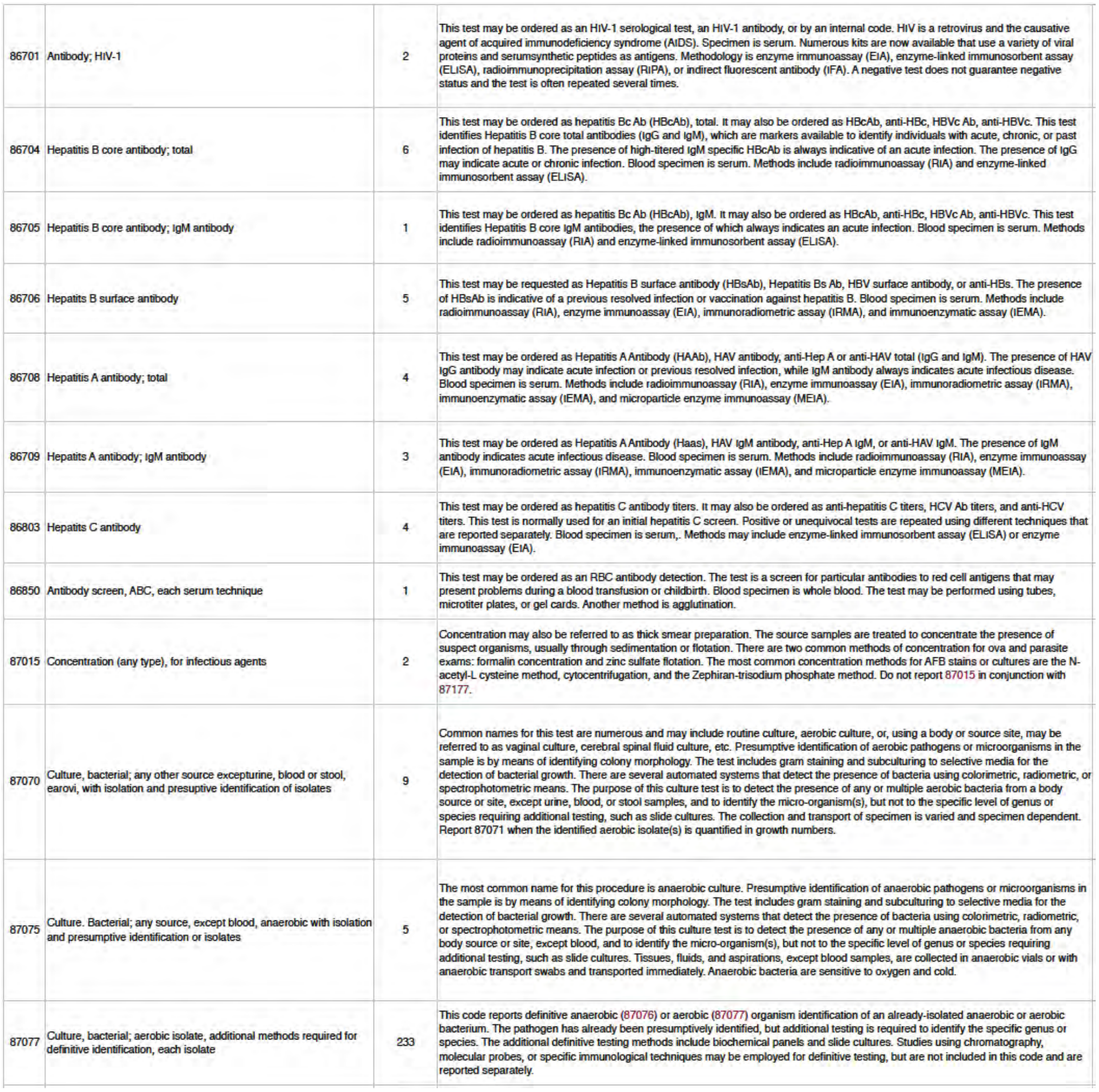
84300	Sodium;serum, plasma or whole blood; urine	71	Sodium is an electrolyte found in extracellular fluid. Blood specimen for serum, plasma, or whole blood sodium (Na) in 84295 is obtained by venipuncture. Methods include atomic absorption spectrometry (AAS), flame emission photometry, and ion-selective electrode (ISE). The specimen for urine Na in 84300 is collected over a 24-hour period or by random urine sample. Methods may include flame emission photometry and ISE. This test is used to identify increased (hypernatremia) and decreased (hyponatremia) levels of sodium due to various conditions or disease states. Report 84302 for a sodium level test done on another source of specimen other than blood serum or urine.
84392	Sulfate, urine	42	This test may be ordered to determine kidney stone risk and in the investigation of sulfur metabolism studies. Sulfates may be measured for the diagnosis of metachromatic leukodystrophy (sulfatide lipidosis), an inherited lipid metabolism that results in the accumulation of metachromatic lipids in the tissues of the central nervous system, leading to paralysis and often death in early adolescence. The specimen is a random or timed urine collection. Method is spectrophotometry.
84402	Testosterone; free	146	These tests may be used to evaluate testosterone levels. Testosterone is an androgenic hormone responsible for, among other biological activities, secondary male characteristics in women. Increased testosterone levels in women may be linked to a variety of conditions, including hirsutism. Code 84403 reports total testosterone, which includes both protein bound and free testosterone. Code 84402 reports testosterone as a free unbound protein. This test may be ordered to assist in diagnosis of hypogonadism, hypopituitarism, and Klinefelter's syndrome, among other disorders. The specimen is serum. Method may be by radioimmunoassay (RIA) and immunoassay (non-isotopic).
84403	Testosterone; total	486	These tests may be used to evaluate testosterone levels. Testosterone is an androgenic hormone responsible for, among other biological activities, secondary male characteristics in women. Increased testosterone levels in women may be linked to a variety of conditions, including hirsutism. Code 84403 reports total testosterone, which includes both protein bound and free testosterone. Code 84402 reports testosterone as a free unbound protein. This test may be ordered to assist in diagnosis of hypogonadism, hypopituitarism, and Klinefelter's syndrome, among other disorders. The specimen is serum. Method may be by radioimmunoassay (RIA) and immunoassay (non-isotopic).
84436	Thyroxine; total	2	This test may be ordered as a T4. The specimen is serum. Methods may include radioimmunoassay (RIA), enzyme-linked immunosorbent assay (ELISA), fluorescence polarization immunoassay (FPIA), and chemiluminescence assay (CIA). The test is performed to determine thyroid function as screening test; total thyroxine makes up approximately 99 percent of the thyroid hormone.
84439	Thyroxine; free	11	This test may be ordered as a FT4, free T4, FTI or FT4 index. The specimen is serum, requiring special handling. Methods may include radioimmunoassay and equilibrium dialysis for reference method. Free thyroxine is a minimal amount of the total T4 level (approximately one percent). This test is not influenced by thyroid-binding abnormalities and perhaps correlates more closely with the true hormonal status. It may be effective in the diagnosis of hyperthyroidism and hypothyroidism.
84443	Thryoid stiumlating hormone (TSH)	23	TSH is produced in the pituitary gland and stimulates the secretion of thyrotropin (T3) and thyroxine (T4); these secretory products monitor TSH. The specimen is serum, requiring special handling. Heel stick or umbilical cord sample is drawn from newborns and may be collected on a special paper. Methods may include radioimmunoassay (RIA), sandwich immunoradiometric assay (IRMA), fluorometric enzyme immunoassay with use of monoclonal antibodies, or microparticle enzyme immunoassay on IMx (MEIA). This test may be performed to determine thyroid function, to differentiate from various types of hypothyroidism (e.g., primary, and pituitary/hypothalamic), or to diagnose hyperthyroidism. The test may be ordered to evaluate therapy in patients receiving hypothyroid treatment, and to detect congenital hypothyroidism
84479	Thryoid hormone (T3 or T4) uptake or thyroid homrone binding ratio	2	This test may be requested as T3 uptake and T4 uptake or THBR. The specimen is serum. Method is chemiluminescent immunoassay
84480	Triiodothyronine T3; total (TT-3)	4	This test may be ordered as a T3 (RIA) or total T3. The specimen is serum. Methods may include radioimmunoassay (RIA), immunochemiluminometric assay, and fluorometric immunoassay. Abnormal results may be diseases and disorders related to the thyroid.
84520	Urea nitrogen; quantitative	147	This test may be requested as blood urea nitrogen (BUN). Urea is an end product of protein metabolism. BUN may be requested to evaluate dehydration or renal function. Blood specimen is serum or plasma. Method is colorimetry, enzymatic, or rate conductivity. This test measures (quantitates) the amount of urea in the blood.
84540	Urea nitrogen; urea	42	This test may provide useful information regarding carbohydrate metabolism (diabetes), kidney function, and acid-base balance, in addition to dietary protein. Urea is a measure of protein breakdown in the body. Urine urea excretion can be measured to obtain a ratio between the plasma (blood) urea and the urine urea; this ratio is an indicator of kidney function. Urine collection over a 24-hour period. Methods may include enzymatic assay, colorimetry, and conductometric.
84550	Uric acid; blood	56	This test may be requested as urate. Uric acid may be ordered to evaluate gout, renal function and a number of other disorders. Blood specimen is serum or plasma. Method is enzymatic or high performance liquid chromatography (HPLC).
84560	Uric acid; other source	68	Uric acid is also known as urate. Methods may include high performance liquid chromatography, uricase, and phosphotungstate. The test may be ordered to determine the possible occurrence of calculus formation, evaluate uric acid in gout, and to identify genetic defects and some malignancies in body fluids other than blood.
84585	Vanilylmlandelic acid (VMA), urine	1	This test is also called 3-methoxy-4-hydroxymandelic acid test, and also as VMA. Urine collection is over a 24-hour period and requires special handling. Methods may include colorimetry, spectrophotometry, gas chromatography, and high performance liquid chromatography (HPLC). The test may be performed to evaluate hypertensive states and to diagnose certain tumors and to monitor the efficacy of treatment modalities.
84702	Gonadotropin, chorionic (hCG); quantitative	39	This test may be ordered as hCG or as a serum pregnancy test. The specimen is serum. Method may be radioimmunoassay (RIA), two-site immunoradiometric assay (IRMA), two-site enzyme-linked immunosorbent assay (ELISA), and radioreceptor assay (RRA). This test is quantitative and measures the amount of hCG present, a determinate of pregnancy and certain tumors.
85014	Blood count; hematocrit	7	This test may be ordered as a hematocrit, Hmt, or Hct. The specimen is whole blood. Method is automated cell counter. The hematocrit or volume of packed red cells (VPRC) in the blood sample is calculated by multiplying the red blood cell count or RBC times the mean corpuscular volume or MCV.
85018	blood count; hemoglobin	1	This test may be ordered as hemoglobin, Hgb, or hemoglobin concentration. The specimen is whole blood. Method is usually automated cell counter but a manual method is seen in labs with a limited test menu and blood bank drawing stations. Hemoglobin is an index of the oxygen-carrying capacity of the blood.
85025	Blood count; automated differential WBC count; completed (CBC), automated	79	This test may be ordered as a complete automated blood count (CBC). The specimen is whole blood. Method is automated cell counter. This code includes the measurement of erythrocytes (red blood cells or RBC), leukocytes (white blood cells or WBC), hemoglobin, hematocrit (volume of packed red blood cells or VPRC), platelet or thrombocyte count, and indices (mean corpuscular hemoglobin or MCH, mean corpuscular hemoglobin concentration or MCHC, mean corpuscular volume or MCV, and red cell distribution width or RDW). Code 85025 includes an automated differential of the white blood cells or "diff" in which the following leukocytes are differentiated: neutrophils or granulocytes, lymphocytes, monocytes, eosinophils, and basophils. Report 85027 if the complete CBC, or automated blood count, is done without the differential WBC count

Exhibit 17



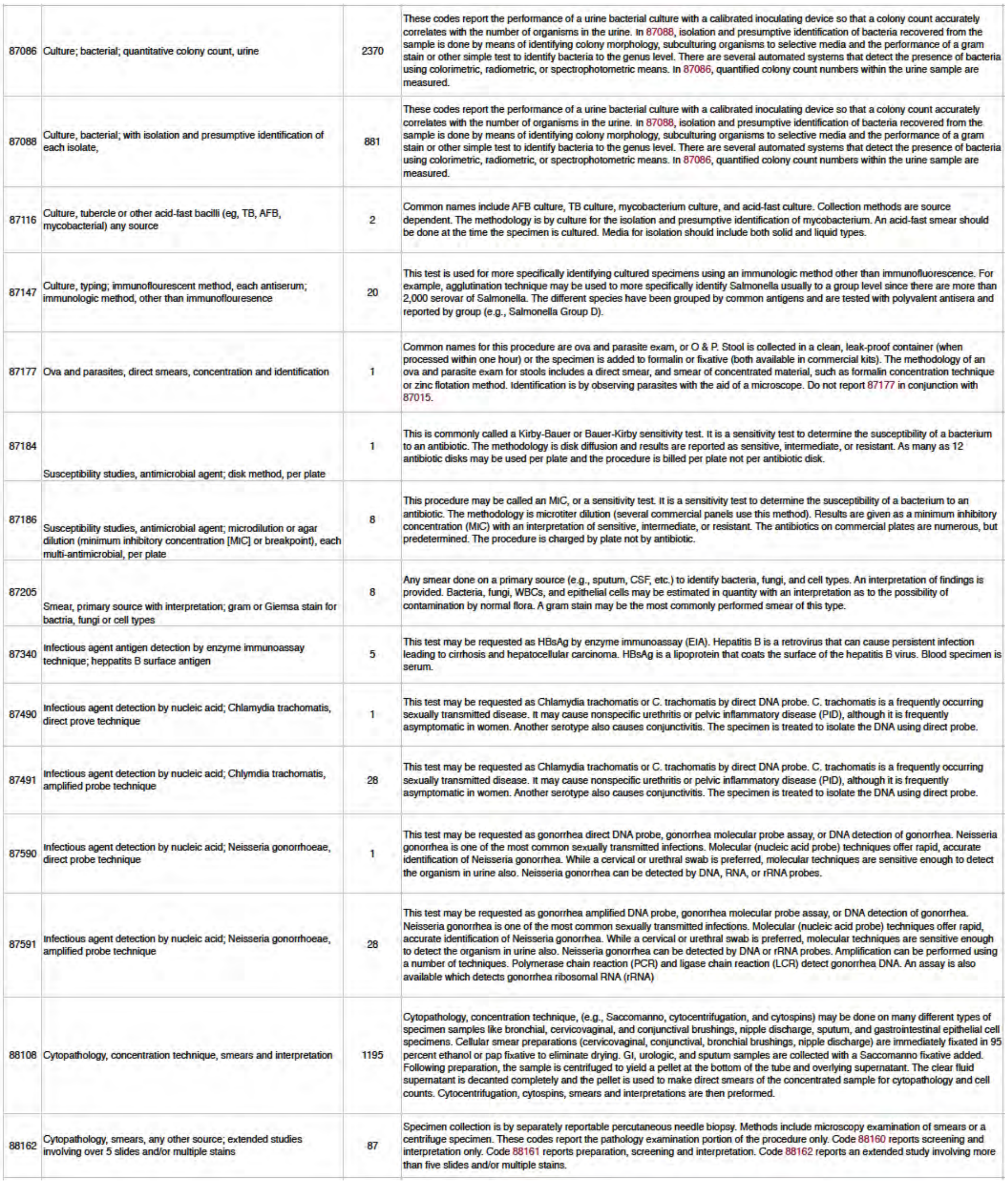
85027	Blood count; compelted (CBC), automated	37	This test may be ordered as a complete automated blood count (CBC). The specimen is whole blood. Method is automated cell counter. This code includes the measurement of erythrocytes (red blood cells or RBC), leukocytes (white blood cells or WBC), hemoglobin, hematocrit (volume of packed red blood cells or VPRC), platelet or thrombocyte count, and indices (mean corpuscular hemoglobin or MCH, mean corpuscular hemoglobin concentration or MCHC, mean corpuscular volume or MCV, and red cell distribution width or RDW). Code 85025 includes an automated differential of the white blood cells or "diff" in which the following leukocytes are differentiated: neutrophils or granulocytes, lymphocytes, monocytes, eosinophils, and basophils. Report 85027 if the complete CBC, or automated blood count, is done without the differential WBC count.
85652	Sedimentation rate, arythrocyte; automated	1	This test may be ordered as a Zeta sedimentation rate or as a Zeta sed rate. Specimen is whole blood. Method is centrifugation; this is an automated test. This test is a non-specific screening test for a number of diseases including anemia, disorders of protein production such as multiple myeloma, and other conditions that alter the size and/or shape of red cells or erythrocytes. This test may also be used to screen diseases that cause an increase or decrease in the amount of protein in the plasma or liquid portion of the blood.
85660	Sickling or RBC, reduction	1	This test may be ordered as a sickle cell metabisulfite test, a sickle cell reduction test, an erythrocyte (RBC) sickling test, or as an RBC reduction sickle cell test. Specimen is whole blood. The method is manual. Whole blood is mixed with a reducing agent that causes erythrocytes that contain abnormal amounts of hemoglobin S to sickle or change their shape to an elongated 'sickle' cell. The solution is examined microscopically and the numbers of sickle cells are reported as a percentage of normal erythrocytes or RBCs.
86301	Immunossay for tumor antigen, quantitative; CA 19-9	1	This test may also be requested as carbohydrate antigen 19-9. The specimen is serum. Method is immunoassay. Quantitative analysis for CA 19-9 is used primarily as a marker for pancreatic cancer. It identifies recurrence and monitors patients. It is also used to monitor gastrointestinal, head/neck, and gynecological cancer. It may identify recurrence of stomach, colorectal, liver, gallbladder, and urothelial malignancies.
86592	Syphillis test, non-treponemal antibody; qualatative	11	This nontreponemal (screening) antibody test is commonly ordered as RPR (rapid plasma reagin), STS (serologic test for syphilis), VDRL (venereal disease research laboratory), or ART (automated reagin test). It may also be ordered as standard test for syphilis. The specimen is serum. The test is commonly used to provide a diagnosis (screening test) for syphilis. The method is by nontreponemal rapid plasma reagin (RPR)-particle agglutination test. More recently, it is being performed by automated methodology, such as enzyme-linked immunosorbent assay (ELISA).
86631	Antibody; Chlamydia	1	This test may be ordered as chlamydia psittaci or LVG titer. The specimen is serum or finger stick in adults, or heel stick in infants. Methods are complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), and immunofluorescent antibody (IFA). This test may be used to determine exposure to chlamydia, though the test should not be used as a specific type. Chlamydomonas is a genus of algae that can cause nongonococcal urethritis, among other infections.
86632	Antibody; Chlamydia, IgM	1	This test may be ordered as chlamydia IgM titer. The specimen is serum or finger stick in adults, or heel stick in infants. Complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), and immunofluorescent antibody (IFA) are methods commonly used to determine previous exposure to chlamydia or a current infection. Chlamydomonas is a genus of algae that can cause nongonococcal urethritis, among other infections.
86689	HTLV or HIV antibody, confirmatory test	13	This test is commonly ordered as HTLV or HIV by Western blot. The specimen is serum. This test may be performed as a confirmation of a positive test for human T cell leukemia II virus or human immunodeficiency virus (HIV), often by a previous enzyme-linked immunoassay (ELISA).
86694	Antibody; herpes simplex, non-specific type	6	These tests may be ordered as HSV antibody titer, HSV titer, herpes simplex antibody titer, or HSV IgG/IGM. The specimen is serum or finger stick in adults, or heel stick in infants. A number of methodologies have been employed, such as complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), indirect fluorescent antibody (IFA), enzyme immunoassay, and latex agglutination. This test has been used as a serologic method to detect previous or recent exposure to herpes simplex. To report non-specific type testing, see 86694; testing for type 1, see 86695; testing for type 2, see 86696.
86695	Antibody; herpes simplex, type 1	20	These tests may be ordered as HSV antibody titer, HSV titer, herpes simplex antibody titer, or HSV IgG/IGM. The specimen is serum or finger stick in adults, or heel stick in infants. A number of methodologies have been employed, such as complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), indirect fluorescent antibody (IFA), enzyme immunoassay, and latex agglutination. This test has been used as a serologic method to detect previous or recent exposure to herpes simplex. To report non-specific type testing, see 86694; testing for type 1, see 86695; testing for type 2, see 86696.
86696	Antibody; herpes simplex, type 2	19	These tests may be ordered as HSV antibody titer, HSV titer, herpes simplex antibody titer, or HSV IgG/IGM. The specimen is serum or finger stick in adults, or heel stick in infants. A number of methodologies have been employed, such as complement fixation (CF), enzyme-linked immunosorbent assay (ELISA), indirect fluorescent antibody (IFA), enzyme immunoassay, and latex agglutination. This test has been used as a serologic method to detect previous or recent exposure to herpes simplex. To report non-specific type testing, see 86694; testing for type 1, see 86695; testing for type 2, see 86696.

Exhibit 17



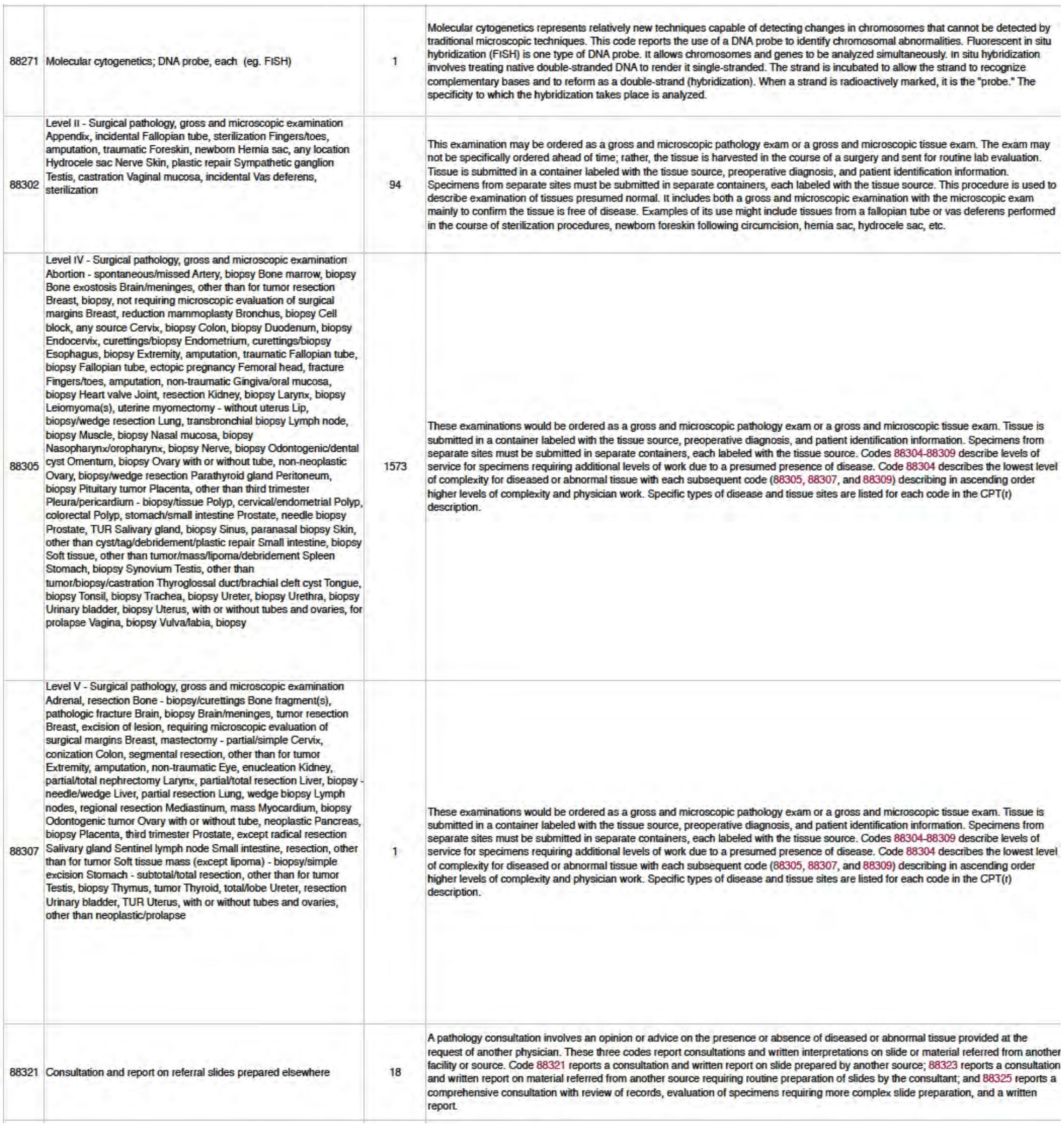
86701	Antibody; HIV-1	2	This test may be ordered as an HIV-1 serological test, an HIV-1 antibody, or by an internal code. HIV is a retrovirus and the causative agent of acquired immunodeficiency syndrome (AIDS). Specimen is serum. Numerous kits are now available that use a variety of viral proteins and serumsynthetic peptides as antigens. Methodology is enzyme immunoassay (EIA), enzyme-linked immunosorbent assay (ELISA), radioimmunoprecipitation assay (RIPA), or indirect fluorescent antibody (IFA). A negative test does not guarantee negative status and the test is often repeated several times.
86704	Hepatitis B core antibody; total	6	This test may be ordered as hepatitis Bc Ab (HBcAb), total. It may also be ordered as HBcAb, anti-HBc, HBVc Ab, anti-HBVc. This test identifies Hepatitis B core total antibodies (IgG and IgM), which are markers available to identify individuals with acute, chronic, or past infection of hepatitis B. The presence of high-titered IgM specific HBcAb is always indicative of an acute infection. The presence of IgG may indicate acute or chronic infection. Blood specimen is serum. Methods include radioimmunoassay (RIA) and enzyme-linked immunosorbent assay (ELISA).
86705	Hepatitis B core antibody; IgM antibody	1	This test may be ordered as hepatitis Bc Ab (HBcAb), IgM. It may also be ordered as HBcAb, anti-HBc, HBVc Ab, anti-HBVc. This test identifies Hepatitis B core IgM antibodies, the presence of which always indicates an acute infection. Blood specimen is serum. Methods include radioimmunoassay (RIA) and enzyme-linked immunosorbent assay (ELISA).
86706	Hepatits B surface antibody	5	This test may be requested as Hepatitis B surface antibody (HBsAb), Hepatitis Bs Ab, HBV surface antibody, or anti-HBs. The presence of HBsAb is indicative of a previous resolved infection or vaccination against hepatitis B. Blood specimen is serum. Methods include radioimmunoassay (RIA), enzyme immunoassay (EIA), immunoradiometric assay (IRMA), and immunoenzymatic assay (IEMA).
86708	Hepatitis A antibody; total	4	This test may be ordered as Hepatitis A Antibody (HAAb), HAV antibody, anti-Hep A or anti-HAV total (IgG and IgM). The presence of HAV IgG antibody may indicate acute infection or previous resolved infection, while IgM antibody always indicates acute infectious disease. Blood specimen is serum. Methods include radioimmunoassay (RIA), enzyme immunoassay (EIA), immunoradiometric assay (IRMA), immunoenzymatic assay (IEMA), and microparticle enzyme immunoassay (MEIA).
86709	Hepatits A antibody; IgM antibody	3	This test may be ordered as Hepatitis A Antibody (Haas), HAV IgM antibody, anti-Hep A IgM, or anti-HAV IgM. The presence of IgM antibody indicates acute infectious disease. Blood specimen is serum. Methods include radioimmunoassay (RIA), enzyme immunoassay (EIA), immunoradiometric assay (IRMA), immunoenzymatic assay (IEMA), and microparticle enzyme immunoassay (MEIA).
86803	Hepatits C antibody	4	This test may be ordered as hepatitis C antibody titers. It may also be ordered as anti-hepatitis C titers, HCV Ab titers, and anti-HCV titers. This test is normally used for an initial hepatitis C screen. Positive or unequivocal tests are repeated using different techniques that are reported separately. Blood specimen is serum,. Methods may include enzyme-linked immunosorbent assay (ELISA) or enzyme immunoassay (EIA).
86850	Antibody screen, ABC, each serum technique	1	This test may be ordered as an RBC antibody detection. The test is a screen for particular antibodies to red cell antigens that may present problems during a blood transfusion or childbirth. Blood specimen is whole blood. The test may be performed using tubes, microtiter plates, or gel cards. Another method is agglutination.
87015	Concentration (any type), for infectious agents	2	Concentration may also be referred to as thick smear preparation. The source samples are treated to concentrate the presence of suspect organisms, usually through sedimentation or flotation. There are two common methods of concentration for ova and parasite exams: formalin concentration and zinc sulfate flotation. The most common concentration methods for AFB stains or cultures are the N-acetyl-L cysteine method, cytocentrifugation, and the Zephiran-trisodium phosphate method. Do not report 87015 in conjunction with 87177.
87070	Culture, bacterial; any other source excepturine, blood or stool, earovi, with isolation and presuptive identification of isolates	9	Common names for this test are numerous and may include routine culture, aerobic culture, or, using a body or source site, may be referred to as vaginal culture, cerebral spinal fluid culture, etc. Presumptive identification of aerobic pathogens or microorganisms in the sample is by means of identifying colony morphology. The test includes gram staining and subculturing to selective media for the detection of bacterial growth. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. The purpose of this culture test is to detect the presence of any or multiple aerobic bacteria from a body source or site, except urine, blood, or stool samples, and to identify the micro-organism(s), but not to the specific level of genus or species requiring additional testing, such as slide cultures. The collection and transport of specimen is varied and specimen dependent. Report 87071 when the identified aerobic isolate(s) is quantified in growth numbers.
87075	Culture. Bacterial; any source, except blood, anaerobic with isolation and presumptive identification or isolates	5	The most common name for this procedure is anaerobic culture. Presumptive identification of anaerobic pathogens or microorganisms in the sample is by means of identifying colony morphology. The test includes gram staining and subculturing to selective media for the detection of bacterial growth. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. The purpose of this culture test is to detect the presence of any or multiple anaerobic bacteria from any body source or site, except blood, and to identify the micro-organism(s), but not to the specific level of genus or species requiring additional testing, such as slide cultures. Tissues, fluids, and aspirations, except blood samples, are collected in anaerobic vials or with anaerobic transport swabs and transported immediately. Anaerobic bacteria are sensitive to oxygen and cold.
87077	Culture, bacterial; aerobic isolate, additional methods required for definitive identification, each isolate	233	This code reports definitive anaerobic (87076) or aerobic (87077) organism identification of an already-isolated anaerobic or aerobic bacterium. The pathogen has already been presumptively identified, but additional testing is required to identify the specific genus or species. The additional definitive testing methods include biochemical panels and slide cultures. Studies using chromatography, molecular probes, or specific immunological techniques may be employed for definitive testing, but are not included in this code and are reported separately.

Exhibit 17



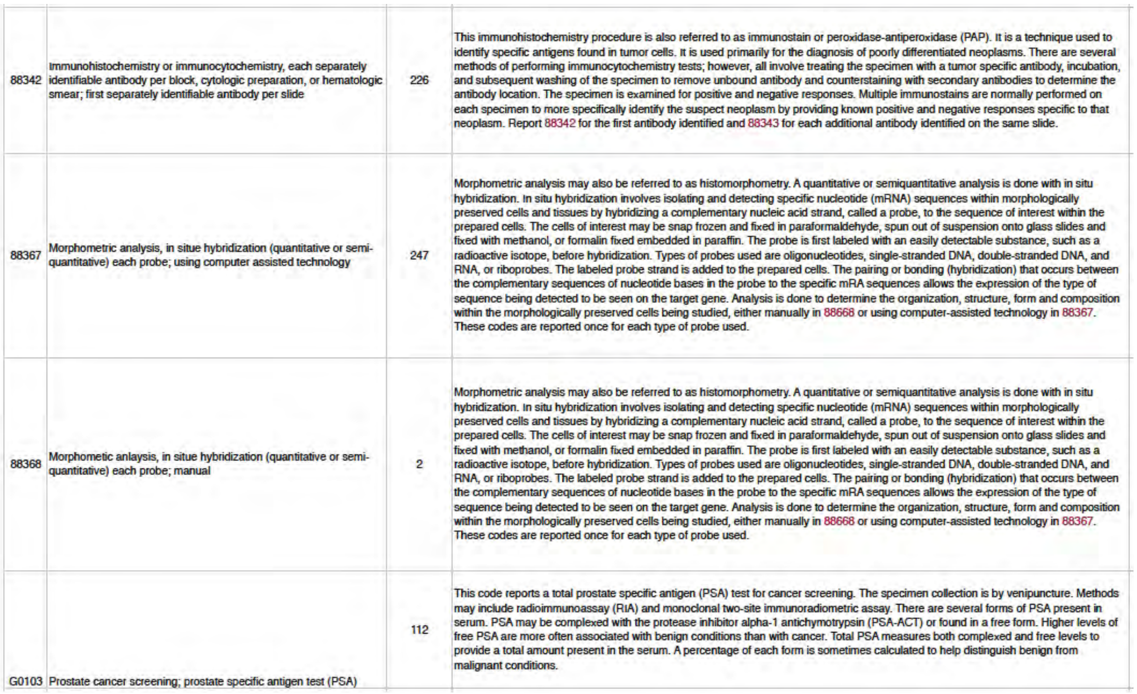
87086	Culture; bacterial; quantitative colony count, urine	2370	These codes report the performance of a urine bacterial culture with a calibrated inoculating device so that a colony count accurately correlates with the number of organisms in the urine. In 87088, isolation and presumptive identification of bacteria recovered from the sample is done by means of identifying colony morphology, subculturing organisms to selective media and the performance of a gram stain or other simple test to identify bacteria to the genus level. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. In 87086, quantified colony count numbers within the urine sample are measured.
87088	Culture, bacterial; with isolation and presumptive identification of each isolate,	881	These codes report the performance of a urine bacterial culture with a calibrated inoculating device so that a colony count accurately correlates with the number of organisms in the urine. In 87088, isolation and presumptive identification of bacteria recovered from the sample is done by means of identifying colony morphology, subculturing organisms to selective media and the performance of a gram stain or other simple test to identify bacteria to the genus level. There are several automated systems that detect the presence of bacteria using colorimetric, radiometric, or spectrophotometric means. In 87086, quantified colony count numbers within the urine sample are measured.
87116	Culture, tubercle or other acid-fast bacilli (eg, TB, AFB, mycobacterial) any source	2	Common names include AFB culture, TB culture, mycobacterium culture, and acid-fast culture. Collection methods are source dependent. The methodology is by culture for the isolation and presumptive identification of mycobacterium. An acid-fast smear should be done at the time the specimen is cultured. Media for isolation should include both solid and liquid types.
87147	Culture, typing; immunoflourescent method, each antiserum; immunologic method, other than immunoflouresence	20	This test is used for more specifically identifying cultured specimens using an immunologic method other than immunofluorescence. For example, agglutination technique may be used to more specifically identify Salmonella usually to a group level since there are more than 2,000 serovar of Salmonella. The different species have been grouped by common antigens and are tested with polyvalent antisera and reported by group (e.g., Salmonella Group D).
87177	Ova and parasites, direct smears, concentration and identification	1	Common names for this procedure are ova and parasite exam, or O & P. Stool is collected in a clean, leak-proof container (when processed within one hour) or the specimen is added to formalin or fixative (both available in commercial kits). The methodology of an ova and parasite exam for stools includes a direct smear, and smear of concentrated material, such as formalin concentration technique or zinc flotation method. Identification is by observing parasites with the aid of a microscope. Do not report 87177 in conjunction with 87015.
87184	Susceptibility studies, antimicrobial agent; disk method, per plate	1	This is commonly called a Kirby-Bauer or Bauer-Kirby sensitivity test. It is a sensitivity test to determine the susceptibility of a bacterium to an antibiotic. The methodology is disk diffusion and results are reported as sensitive, intermediate, or resistant. As many as 12 antibiotic disks may be used per plate and the procedure is billed per plate not per antibiotic disk.
87186	Susceptibility studies, antimicrobial agent; microdilution or agar dilution (minimum inhibitory concentration [MIC] or breakpoint), each multi-antimicrobial, per plate	8	This procedure may be called an MIC, or a sensitivity test. It is a sensitivity test to determine the susceptibility of a bacterium to an antibiotic. The methodology is microtiter dilution (several commercial panels use this method). Results are given as a minimum inhibitory concentration (MIC) with an interpretation of sensitive, intermediate, or resistant. The antibiotics on commercial plates are numerous, but predetermined. The procedure is charged by plate not by antibiotic.
87205	Smear, primary source with interpretation; gram or Giemsa stain for bactria, fungi or cell types	8	Any smear done on a primary source (e.g., sputum, CSF, etc.) to identify bacteria, fungi, and cell types. An interpretation of findings is provided. Bacteria, fungi, WBCs, and epithelial cells may be estimated in quantity with an interpretation as to the possibility of contamination by normal flora. A gram stain may be the most commonly performed smear of this type.
87340	Infectious agent antigen detection by enzyme immunoassay technique; heppatits B surface antigen	5	This test may be requested as HBsAg by enzyme immunoassay (EIA). Hepatitis B is a retrovirus that can cause persistent infection leading to cirrhosis and hepatocellular carcinoma. HBsAg is a lipoprotein that coats the surface of the hepatitis B virus. Blood specimen is serum.
87490	Infectious agent detection by nucleic acid; Chlamydia trachomatis, direct prove technique	1	This test may be requested as Chlamydia trachomatis or C. trachomatis by direct DNA probe. C. trachomatis is a frequently occurring sexually transmitted disease. It may cause nonspecific urethritis or pelvic inflammatory disease (PID), although it is frequently asymptomatic in women. Another serotype also causes conjunctivitis. The specimen is treated to isolate the DNA using direct probe.
87491	Infectious agent detection by nucleic acid; Chlymdia trachomatis, amplified probe technique	28	This test may be requested as Chlamydia trachomatis or C. trachomatis by direct DNA probe. C. trachomatis is a frequently occurring sexually transmitted disease. It may cause nonspecific urethritis or pelvic inflammatory disease (PID), although it is frequently asymptomatic in women. Another serotype also causes conjunctivitis. The specimen is treated to isolate the DNA using direct probe.
87590	Infectious agent detection by nucleic acid; Neisseria gonorrhoeae, direct probe technique	1	This test may be requested as gonorrhea direct DNA probe, gonorrhea molecular probe assay, or DNA detection of gonorrhea. Neisseria gonorrhea is one of the most common sexually transmitted infections. Molecular (nucleic acid probe) techniques offer rapid, accurate identification of Neisseria gonorrhea. While a cervical or urethral swab is preferred, molecular techniques are sensitive enough to detect the organism in urine also. Neisseria gonorrhea can be detected by DNA, RNA, or rRNA probes.
87591	Infectious agent detection by nucleic acid; Neisseria gonorrhoeae, amplified probe technique	28	This test may be requested as gonorrhea amplified DNA probe, gonorrhea molecular probe assay, or DNA detection of gonorrhea. Neisseria gonorrhea is one of the most common sexually transmitted infections. Molecular (nucleic acid probe) techniques offer rapid, accurate identification of Neisseria gonorrhea. While a cervical or urethral swab is preferred, molecular techniques are sensitive enough to detect the organism in urine also. Neisseria gonorrhea can be detected by DNA or rRNA probes. Amplification can be performed using a number of techniques. Polymerase chain reaction (PCR) and ligase chain reaction (LCR) detect gonorrhea DNA. An assay is also available which detects gonorrhea ribosomal RNA (rRNA)
88108	Cytopathology, concentration technique, smears and interpretation	1195	Cytopathology, concentration technique, (e.g., Saccomanno, cytocentrifugation, and cytospins) may be done on many different types of specimen samples like bronchial, cervicovaginal, and conjunctival brushings, nipple discharge, sputum, and gastrointestinal epithelial cell specimens. Cellular smear preparations (cervicovaginal, conjunctival, bronchial brushings, nipple discharge) are immediately fixated in 95 percent ethanol or pap fixative to eliminate drying. GI, urologic, and sputum samples are collected with a Saccomanno fixative added. Following preparation, the sample is centrifuged to yield a pellet at the bottom of the tube and overlying supernatant. The clear fluid supernatant is decanted completely and the pellet is used to make direct smears of the concentrated sample for cytopathology and cell counts. Cytocentrifugation, cytospins, smears and interpretations are then preformed.
88162	Cytopathology, smears, any other source; extended studies involving over 5 slides and/or multiple stains	87	Specimen collection is by separately reportable percutaneous needle biopsy. Methods include microscopy examination of smears or a centrifuge specimen. These codes report the pathology examination portion of the procedure only. Code 88160 reports screening and interpretation only. Code 88161 reports preparation, screening and interpretation. Code 88162 reports an extended study involving more than five slides and/or multiple stains.

Exhibit 17



88271	Molecular cytogenetics; DNA probe, each (eg. FISH)	1	Molecular cytogenetics represents relatively new techniques capable of detecting changes in chromosomes that cannot be detected by traditional microscopic techniques. This code reports the use of a DNA probe to identify chromosomal abnormalities. Fluorescent in situ hybridization (FISH) is one type of DNA probe. It allows chromosomes and genes to be analyzed simultaneously. In situ hybridization involves treating native double-stranded DNA to render it single-stranded. The strand is incubated to allow the strand to recognize complementary bases and to reform as a double-strand (hybridization). When a strand is radioactively marked, it is the "probe." The specificity to which the hybridization takes place is analyzed.
88302	Level II - Surgical pathology, gross and microscopic examination Appendix, incidental Fallopian tube, sterilization Fingers/toes, amputation, traumatic Foreskin, newborn Hernia sac, any location Hydrocele sac Nerve Skin, plastic repair Sympathetic ganglion Testis, castration Vaginal mucosa, incidental Vas deferens, sterilization	94	This examination may be ordered as a gross and microscopic pathology exam or a gross and microscopic tissue exam. The exam may not be specifically ordered ahead of time; rather, the tissue is harvested in the course of a surgery and sent for routine lab evaluation. Tissue is submitted in a container labeled with the tissue source, preoperative diagnosis, and patient identification information. Specimens from separate sites must be submitted in separate containers, each labeled with the tissue source. This procedure is used to describe examination of tissues presumed normal. It includes both a gross and microscopic examination with the microscopic exam mainly to confirm the tissue is free of disease. Examples of its use might include tissues from a fallopian tube or vas deferens performed in the course of sterilization procedures, newborn foreskin following circumcision, hernia sac, hydrocele sac, etc.
88305	Level IV - Surgical pathology, gross and microscopic examination Abortion - spontaneous/missed Artery, biopsy Bone marrow, biopsy Bone exostosis Brain/meninges, other than for tumor resection Breast, biopsy, not requiring microscopic evaluation of surgical margins Breast, reduction mammoplasty Bronchus, biopsy Cell block, any source Cervix, biopsy Colon, biopsy Duodenum, biopsy Endocervix, curettings/biopsy Endometrium, curettings/biopsy Esophagus, biopsy Extremity, amputation, traumatic Fallopian tube, biopsy Fallopian tube, ectopic pregnancy Femoral head, fracture Fingers/toes, amputation, non-traumatic Gingiva/oral mucosa, biopsy Heart valve Joint, resection Kidney, biopsy Larynx, biopsy Leiomyoma(s), uterine myomectomy - without uterus Lip, biopsy/wedge resection Lung, transbronchial biopsy Lymph node, biopsy Muscle, biopsy Nasal mucosa, biopsy Nasopharynx/oropharynx, biopsy Nerve, biopsy Odontogenic/dental cyst Omentum, biopsy Ovary with or without tube, non-neoplastic Ovary, biopsy/wedge resection Parathyroid gland Peritoneum, biopsy Pituitary tumor Placenta, other than third trimester Pleura/pericardium - biopsy/tissue Polyp, cervical/endometrial Polyp, colorectal Polyp, stomach/small intestine Prostate, needle biopsy Prostate, TUR Salivary gland, biopsy Sinus, paranasal biopsy Skin, other than cyst/tag/debridement/plastic repair Small intestine, biopsy Soft tissue, other than tumor/mass/lipoma/debridement Spleen Stomach, biopsy Synovium Testis, other than tumor/biopsy/castration Thyroglossal duct/brachial cleft cyst Tongue, biopsy Tonsil, biopsy Trachea, biopsy Ureter, biopsy Urethra, biopsy Urinary bladder, biopsy Uterus, with or without tubes and ovaries, for prolapse Vagina, biopsy Vulva/labia, biopsy	1573	These examinations would be ordered as a gross and microscopic pathology exam or a gross and microscopic tissue exam. Tissue is submitted in a container labeled with the tissue source, preoperative diagnosis, and patient identification information. Specimens from separate sites must be submitted in separate containers, each labeled with the tissue source. Codes 88304-88309 describe levels of service for specimens requiring additional levels of work due to a presumed presence of disease. Code 88304 describes the lowest level of complexity for diseased or abnormal tissue with each subsequent code (88305, 88307, and 88309) describing in ascending order higher levels of complexity and physician work. Specific types of disease and tissue sites are listed for each code in the CPT(r) description.
88307	Level V - Surgical pathology, gross and microscopic examination Adrenal, resection Bone - biopsy/curettings Bone fragment(s), pathologic fracture Brain, biopsy Brain/meninges, tumor resection Breast, excision of lesion, requiring microscopic evaluation of surgical margins Breast, mastectomy - partial/simple Cervix, conization Colon, segmental resection, other than for tumor Extremity, amputation, non-traumatic Eye, enucleation Kidney, partial/total nephrectomy Larynx, partial/total resection Liver, biopsy - needle/wedge Liver, partial resection Lung, wedge biopsy Lymph nodes, regional resection Mediastinum, mass Myocardium, biopsy Odontogenic tumor Ovary with or without tube, neoplastic Pancreas, biopsy Placenta, third trimester Prostate, except radical resection Salivary gland Sentinel lymph node Small intestine, resection, other than for tumor Soft tissue mass (except lipoma) - biopsy/simple excision Stomach - subtotal/total resection, other than for tumor Testis, biopsy Thymus, tumor Thyroid, total/lobe Ureter, resection Urinary bladder, TUR Uterus, with or without tubes and ovaries, other than neoplastic/prolapse	1	These examinations would be ordered as a gross and microscopic pathology exam or a gross and microscopic tissue exam. Tissue is submitted in a container labeled with the tissue source, preoperative diagnosis, and patient identification information. Specimens from separate sites must be submitted in separate containers, each labeled with the tissue source. Codes 88304-88309 describe levels of service for specimens requiring additional levels of work due to a presumed presence of disease. Code 88304 describes the lowest level of complexity for diseased or abnormal tissue with each subsequent code (88305, 88307, and 88309) describing in ascending order higher levels of complexity and physician work. Specific types of disease and tissue sites are listed for each code in the CPT(r) description.
88321	Consultation and report on referral slides prepared elsewhere	18	A pathology consultation involves an opinion or advice on the presence or absence of diseased or abnormal tissue provided at the request of another physician. These three codes report consultations and written interpretations on slide or material referred from another facility or source. Code 88321 reports a consultation and written report on slide prepared by another source; 88323 reports a consultation and written report on material referred from another source requiring routine preparation of slides by the consultant; and 88325 reports a comprehensive consultation with review of records, evaluation of specimens requiring more complex slide preparation, and a written report.

Exhibit 17



88342	Immunohistochemistry or immunocytochemistry, each separately identifiable antibody per block, cytologic preparation, or hematologic smear; first separately identifiable antibody per slide	226	This immunohistochemistry procedure is also referred to as immunostain or peroxidase-antiperoxidase (PAP). It is a technique used to identify specific antigens found in tumor cells. It is used primarily for the diagnosis of poorly differentiated neoplasms. There are several methods of performing immunocytochemistry tests; however, all involve treating the specimen with a tumor specific antibody, incubation, and subsequent washing of the specimen to remove unbound antibody and counterstaining with secondary antibodies to determine the antibody location. The specimen is examined for positive and negative responses. Multiple immunostains are normally performed on each specimen to more specifically identify the suspect neoplasm by providing known positive and negative responses specific to that neoplasm. Report 88342 for the first antibody identified and 88343 for each additional antibody identified on the same slide.
88367	Morphometric analysis, in situe hybridization (quantitative or semi-quantitative) each probe; using computer assisted technology	247	Morphometric analysis may also be referred to as histomorphometry. A quantitative or semiquantitative analysis is done with in situ hybridization. In situ hybridization involves isolating and detecting specific nucleotide (mRNA) sequences within morphologically preserved cells and tissues by hybridizing a complementary nucleic acid strand, called a probe, to the sequence of interest within the prepared cells. The cells of interest may be snap frozen and fixed in paraformaldehyde, spun out of suspension onto glass slides and fixed with methanol, or formalin fixed embedded in paraffin. The probe is first labeled with an easily detectable substance, such as a radioactive isotope, before hybridization. Types of probes used are oligonucleotides, single-stranded DNA, double-stranded DNA, and RNA, or riboprobes. The labeled probe strand is added to the prepared cells. The pairing or bonding (hybridization) that occurs between the complementary sequences of nucleotide bases in the probe to the specific mRA sequences allows the expression of the type of sequence being detected to be seen on the target gene. Analysis is done to determine the organization, structure, form and composition within the morphologically preserved cells being studied, either manually in 88668 or using computer-assisted technology in 88367. These codes are reported once for each type of probe used.
88368	Morphometic anlaysis, in situe hybridization (quantitative or semi-quantitative) each probe; manual	2	Morphometric analysis may also be referred to as histomorphometry. A quantitative or semiquantitative analysis is done with in situ hybridization. In situ hybridization involves isolating and detecting specific nucleotide (mRNA) sequences within morphologically preserved cells and tissues by hybridizing a complementary nucleic acid strand, called a probe, to the sequence of interest within the prepared cells. The cells of interest may be snap frozen and fixed in paraformaldehyde, spun out of suspension onto glass slides and fixed with methanol, or formalin fixed embedded in paraffin. The probe is first labeled with an easily detectable substance, such as a radioactive isotope, before hybridization. Types of probes used are oligonucleotides, single-stranded DNA, double-stranded DNA, and RNA, or riboprobes. The labeled probe strand is added to the prepared cells. The pairing or bonding (hybridization) that occurs between the complementary sequences of nucleotide bases in the probe to the specific mRA sequences allows the expression of the type of sequence being detected to be seen on the target gene. Analysis is done to determine the organization, structure, form and composition within the morphologically preserved cells being studied, either manually in 88668 or using computer-assisted technology in 88367. These codes are reported once for each type of probe used.
G0103	Prostate cancer screening; prostate specific antigen test (PSA)	112	This code reports a total prostate specific antigen (PSA) test for cancer screening. The specimen collection is by venipuncture. Methods may include radioimmunoassay (RIA) and monoclonal two-site immunoradiometric assay. There are several forms of PSA present in serum. PSA may be complexed with the protease inhibitor alpha-1 antichymotrypsin (PSA-ACT) or found in a free form. Higher levels of free PSA are more often associated with benign conditions than with cancer. Total PSA measures both complexed and free levels to provide a total amount present in the serum. A percentage of each form is sometimes calculated to help distinguish benign from malignant conditions.

Exhibit 17

Exhibit 18

In the Matter of:

LabMD, Inc.

January 17, 2014
Jerry Maxey

Condensed Transcript with Word Index

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

Exhibit 18

MS. MORGAN: Objection: Calls for speculation.

A. Not to my knowledge, no one physical.

MS. COX: I think we should take a short break, if we could go off the record for maybe five minutes.

(A break was taken.)

Q. (By Ms. Cox) Okay. So we can go back on the record, please. I'm sorry.

A. I did remember something about the South Haven PCs.

Q. Yes.

A. I remembered asking my IT person, my ultrasonographer, to remove all LabMD PCs from South Haven and the Memphis office, and he did go down to South Haven and bring the LabMD PCs up to our Memphis office. And we have them stored in a bay right now.

Q. When did that happen?

A. When we quit using LabMD.

Q. Okay.

A. So I forgot that.

Q. Thank you. Now I would like to ask you about Sun's communications to its patients.

A. Uh-huh.

Q. Do you know what information Sun conveys to its patients regarding how specimens would be tested?

A. No. If -- no.

Q. Would Sun ever communicate to patients that their specimens were going to go to LabMD?

A. No. We just inform them that it's going to an outside lab. Different insurances have specific labs that would go to different places. The patient was just concerned that it went to the right lab that was considered the network for their plan.

Q. So a patient would not know which lab was testing their specimen?

A. That's correct, except if they knew that if their insurance -- a specific request was for Aetna. But if someone had another insurance plan that was not lab specific, they wouldn't know.

Q. And the patient, when would the patient find out perhaps when their insurance company -- which lab tested their specimen?

MS. MORGAN: Objection: Calls for speculation.

A. I would imagine they would get a bill from LabMD if their insurance did not pay.

Q. (By Ms. Cox) So after it had been tested by that lab?

A. That's correct.

Q. And so the patient could not know what the lab's data security practices were before their specimen was sent?

A. No.

Q. Did Sun advise its patients that its patients' demographic data would be sent to LabMD even if no specimen was taken?

A. No. The reason being as all providers of medical services, even calling the hospital to send patients over for labs, send people to diagnostic labs for x-rays and things of that nature is custom to provide that information to those entities so they can identify the patient as coming in their door for services that are needed. And that is information they request as well, the insurance information, the patient demographic information.

So we accommodated those entities, hospitals, diagnostic labs, independent labs, reference labs with their information because they were providing medical services for the patients.

And I imagine when the patients got to those lab places, they would be informed of the policies of the insurance and things of that nature. But that's something that we as healthcare providers -- we provide to other healthcare providers, is the basic information and diagnoses for treatment.

Q. I believe earlier you testified that the Sun server would transmit all information hourly to the LabMD server in Atlanta; correct?

A. That was my layman understanding of the process.

Q. So that would be all patient data on Sun's server?

A. Only confined to the patient demographic and the insurance information, not any of the medical records per se or progress notes, etc.

Q. So a patient who wasn't having a LabMD specimen, it was -- their information, their demographic information, could still be transferred to the LabMD server?

A. That's correct, as far as my understanding goes.

Q. That patient would not know that LabMD had their demographic information?

Exhibit 18

EXHIBIT 19

In the Matter of:

LabMD, Inc.

February 4, 2014
Letonya Randolph

Condensed Transcript with Word Index

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

Exhibit 19

65

install and configure firewalls on the LabMD hardware used to transmit and receive information from LabMD?

A. We were relying on LabMD to service and update all of their hardware that they provided to us.

Q. Now I'd like to ask you about risk assessments that might have been done.

Did LabMD perform any risk assessments on how its computers and servers worked with Midtown's server and network?

MS. HARRIS: Objection, vague as to risk assessment, may call for an expert conclusion.

Q. (By Ms. Cox) You may answer.

A. Not to my knowledge.

Q. Now I would like to ask you about the operating systems on the LabMD computers.

What operating system did the LabMD computers use? Was it a Windows operating system on the LabMD computers?

A. Yes.

Q. Do you know what version of Windows the LabMD machines used?

A. Unsure.

Q. Do you recall the operating system changing versions over time at all?

A. Unsure. I think it may have been Windows

66

XP.

Q. Do you recall a time where there was a change in how the desktop looked or any big changes in the layout of the computer's desktop?

A. No, always looked the same.

Q. While Midtown was a LabMD client, did LabMD use any outside security contractors to help maintain the computer equipment at Midtown?

MS. HARRIS: Objection, calls for speculation, lacks foundation.

THE WITNESS: Not to my knowledge.

Q. (By Ms. Cox) Now I'd like to discuss Midtown's communications to its patients.

What information did Midtown convey to its patients about how the patients' specimens would be tested?

A. Midtown generally did not convey any information other than telling the patients that their lab work would be sent to LabMD. If the patient asked, lab work we sent to LabMD, and that's it.

Q. And the patient would have to inquire for Midtown to inform the patient that their specimen was going to LabMD?

A. No.

Q. Midtown would inform the patient

67

proactively that the --

A. No. We just -- patients never asked, and we never offered that information. We just sent -- we just sent the -- our specimens to LabMD unless the patient requested that their specimen be sent to a different lab, mainly a lab that was contracted through their insurance.

Q. How often would a patient inquire about where their specimen was going?

A. Infrequent, maybe two or three times -- two or three times a month. Within the past few years, more often.

Q. So is it fair to say the great majority of patients did not know their specimen was going to LabMD?

A. Yes.

Q. So is it fair to say that the patient would not know what LabMD's data security practices were?

A. Yes.

Q. From the way you described the flow of data from Centricity to LabMD, so that when you order a test, the information would pre-populate when you entered a Midtown Urology patient identifier number, is it fair to say that all of Midtown's patients'

68

information flowed to LabMD's server?

MS. HARRIS: Objection, misstates the testimony.

THE WITNESS: I am unsure. I'm unsure.

Q. (By Ms. Cox) If a patient was not having a specimen tested but you were to -- if a patient did not have a specimen drawn, if you were to put in their patient identifier name in the LabMD software, would their information come up?

MS. HARRIS: Objection, vague and ambiguous.

THE WITNESS: Unsure. We -- with the exception of ordering a test, we have no reason to put information into LabMD. We have no reason to do that, so I am unsure if we were to put information, patient's information into the system, if that information would come up in LabMD's system. I am unsure.

Q. (By Ms. Cox) So if you were to collect a specimen and then attempt to order the test, I believe you testified earlier that the patient's information, if it didn't pre-populate immediately, it would usually in the next hour or so or you would try before the end of the day and it would be there?

A. Yes.

Exhibit 19

EXHIBIT 20

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

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

REBUTTAL EXPERT REPORT OF CLAY SHIELDS, PH.D.

Exhibit 20

TABLE OF CONTENTS

Exhibit 20

Exhibit 20

REBUTTAL EXPERT REPORT OF CLAY SHIELDS, PH.D.

I. Introduction

1. I am a tenured full Professor in the Computer Science Department at Georgetown University, with expertise in networking and network protocols, computer security, digital forensics, and responding to network and computer system events.

2. The FTC has engaged me to testify as a rebuttal expert in this litigation. Complaint Counsel has asked me to review the report of Adam Fisk and provide opinions about Mr. Fisk's conclusions concerning the LimeWire peer-to-peer file sharing program and the disclosure of a LabMD file containing sensitive information about approximately 9,300 individuals on a peer-to-peer file sharing network (this file is known alternatively as the "insuranceaging_6.05.071.pdf" file and the "1,718 File"). In particular, as explained in more detail in Section V below, Complaint Counsel has asked me to:

a. Explain generally how peer-to-peer (p2p) networks and programs work;

b. Provide an opinion responding to Mr. Fisk's discussion of how the 1,718 file was made available to the Gnutella p2p network;

c. Evaluate Mr. Fisk's opinion that limitations of LimeWire's search functionality made it "extremely unlikely" that a typical LimeWire user could have found the 1,718 File and downloaded it from LabMD;[1]

d. Evaluate Mr. Fisk's opinion that "casual LimeWire users" could not find the 1,718 File using other methods and that only "sophisticated organizations capable of

[1] Fisk Report, p. 16, 23.

Exhibit 20

deploying the financial and ultimately technical resources required" could locate the 1,718 File;[2] and

e. Evaluate Mr. Fisk's opinion that a thumb drive or email was likely to have been used to transfer the 1,718 File to a computer outside LabMD, from where it was downloaded to a p2p network.[3]

3. Based on my review of Mr. Fisk's report, materials contained therein, and the materials described in Section IV, below, and my experience described in Section II, below, I conclude that the 1,718 File was most likely shared inadvertently and disagree with certain of Mr. Fisk's opinions. In Section V, below, I present my specific opinions that support my conclusion.

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

a. A summary of my experience and qualifications (Section II);

b. An overview of the operation of peer-to-peer networks and programs (Section III);

c. A description of the materials that I considered in forming my opinions and conclusions (Section IV); and

d. My evaluation of some of Mr. Fisk's opinions (Section V).

II. Summary of Experience and Qualifications

5. I have over 20 years of computer science experience, including my time spent earning Ph.D. and Master's degrees in Computer Engineering from UC Santa Cruz. Prior to that, I earned a bachelor's degree in Electrical Engineering from the University of Virginia. My Ph.D. dissertation was in the area of computer networking as well as network and computer security, and I have since become involved in digital forensics research, the goal of which is to improve

[2] Fisk Report, p. 25.
[3] Fisk Report, p. 25.

Exhibit 20

how security professionals respond to digital crime and misuse. I have expertise in developing and analyzing network protocols as well as investigating and responding to events on networks and computer systems.

6. Throughout my academic career, my research has focused on issues in network and computer security, revolving around users who are attempting to conceal their identity on the network. The goal of this research is to provide security and privacy through anonymity for individual users while allowing authorities to locate network attackers and arrest criminals. I have had ten papers published in refereed journals. I have published more than twenty reviewed conference and workshop papers, primarily in high-quality Association of Computing Machinery and Institute of Electrical and Electronics Engineers venues with low acceptance rates, including work that won an outstanding paper award. My research is or has been supported by peer-reviewed grants from the National Science Foundation, the Department of Justice, the Naval Postgraduate School, and the Defense Advanced Research Projects Agency. I have been primary investigator or co-primary investigator on over three million dollars in research funding.

7. My initial research was on how to allow effective multi-party communication using a technology known as multicast. Later, my research focused on systems for providing anonymity to users through p2p technology and I collaboratively made many advances in this area, including helping to detail an attack against The Onion Router (TOR) network that lead to changes in how TOR works. I have also conducted work in a variety of other areas relating to the security of computer networks, including covert channels used to smuggle data out of networks and secure wireless protocols.

8. More recently, I have moved my research into the area of digital forensics. This discipline attempts to identify evidence to support or refute hypotheses about user actions based

Exhibit 20

on the evidence available as a part of normal computer system operation. I received extensive commercial training in the area, and earned a designation and an EnCase Certified Examiner. For a period, I ran a small business alongside my academic work in which I conducted forensic examinations. I have received three patents on a novel area of digital forensics, and collaboratively released a software tool named RoundUp that has gained wide acceptance in the law enforcement community. I have also released a tool named sdtext that allows investigators to identify similar files from a set of evidence. I served for two years as the program chair of one of the leading conferences on forensics, the Digital Forensics Research Conference, and was in charge of conducting peer review of the submitted papers. I have served as a reviewer for a number of other security and forensics conferences, and as a reviewer for a number of journals in those areas.

9. As part of my forensics research I have been involved in a collaborative effort that resulted in the development of a tool that is widely used by law enforcement to investigate the sharing of child sexual abuse images using the Gnutella network. RoundUp is a modified Gnutella client (or program) in use by various police forces to locate and create warrants for arrest for individuals sharing child pornography online. In August 2010, RoundUp was declared part of the US National Strategy for Child Exploitation Prevention and Interdiction. As of August 2010, RoundUp was being used by over 1,224 individual investigators and 58 Internet Crimes Against Children Task Forces. I am experienced in how Gnutella operates and what evidence it generates.

10. I have taught courses at the graduate level in Computer Security and in Network Security, as well as a course in Operating Systems. At the undergraduate level, I have taught courses in computer and network security (collectively referred to as Information Assurance); in computer

Exhibit 20

networking; in operating systems; and in an introduction to programming. I have one of the highest overall teaching scores in my department, and have twice been nominated for the Dean's Teaching Award. I led Georgetown University's successful effort to be declared an NSA Center of Excellence in Information Assurance Education.

11. A more extensive summary of my professional accomplishments, and a list of all publications that I have authored within the last 15 years can be found in my *curriculum vitae*, a copy of which is attached to this report as Appendix A.

12. I am being compensated at a rate of $300 per hour for my work in connection with this litigation.

III. Overview of the Operation of Peer-to Peer Networks and Programs

A. A Simple Overview of Gnutella/LimeWire Operation

13. In this section, I describe at a high level the operation of p2p networks using the Gnutella p2p searching protocol and the LimeWire p2p program. Although my description could proceed using other p2p file sharing programs that operate on the Gnutella network, I am using LimeWire because LimeWire was the p2p program that was found on the LabMD computer used by the company's billing manager.[4]

14. LimeWire is a program that allows users to share files with other people who are using another network-connected computer and who are running similar software. This might be another copy of LimeWire or one of the many other programs that also connects to the Gnutella network. LimeWire and other p2p programs are often used to share music, videos, pictures, and other materials.

[4] LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶¶ 40-41.

Exhibit 20

15. The Gnutella network consists of all the computers, referred to commonly as peers or nodes, that are running a program like LimeWire to communicate over the Internet and participate in the Gnutella protocol. It is this collaborative nature of communication in which all nodes are essentially participating equally that leads it to being called a peer-to-peer network. This is in contrast to another common, more centralized model, called client-server, in which there are specialized servers that exist to answer queries from simpler clients. Web sites that respond to requests from web browsers are a common example of this model of communication.

16. It is worthwhile to note that in p2p networks it is very common for nodes to join and leave the network often, as the computer is shutdown or restarted or the software is stopped. This is in contrast to client-server models in which the servers are expected to be constantly available.

17. Gnutella programs, like LimeWire, are configured to offer a particular set of files for sharing. This is typically done when the program is installed and requires the user to select a directory or set of directories on the local file system to share. The selection of these directories can also be changed once the program is installed. Once these directories are selected, the contents are made freely available for sharing with other users of the network.

18. Typically, users will search using terms related to the particular file they hope to find and receive a list of possible matches. They then choose which file they want to download from the list. This file is then downloaded from other peers who possess that file. In the case where many peers have a copy of the file, it is common to download small pieces of the file from many different peers and reassemble the pieces. This speeds file transfer by allowing use of the resources of many peers simultaneously.

19. The peer is able to verify that the file was received correctly because the search results which are returned include a cryptographic hash of the file. A hash is a long number computed

Exhibit 20

based on all the data that makes up the file and is statistically unique to that file and which is essentially impossible to forge. A peer can compute the hash of the file when it is assembled and verify that the overall download is correct.

20. It is common, though not required, for the folder that receives downloads from the network to also be the folder that contains the files that the user is sharing with others. Files that are downloaded into the shared directory, described above, then become available for others to download.

21. Once a file has been downloaded by another computer in the p2p network it can be shared by that computer without downloading it again from the original computer. Accordingly, once a file has been shared on a p2p network it can be difficult or impossible to remove it from the network.

22. In summary, users of the file sharing network make available files that others can come and take. They do so by selecting one or more directories on their computers that will contain the files they will share and intentionally or inadvertently putting files in these directories and making these files available to the file-sharing network.

B. Search in Gnutella

23. In the original Gnutella network, each peer participated in receiving and forwarding search queries. A user would initiate a search request by choosing some search criteria. The Gnutella software running on the user’s computer would then create and send a search request using that criteria. A peer that received a query would forward it on to all the other peers to which it was connected, each time it was forwarded being called a “hop." Each query would travel only a set number of hops before expiring. A peer that had a file that matched the query would then send a reply back to the requestor. The user could then review the search responses

Exhibit 20

and could choose to download one of the files. The user's p2p software would then connect directly to the computer that had the desired file for download. This operation is common knowledge, and is detailed in the Gnutella 0.4 specifications, available from http://rfc-gnutella.sourceforge.net/developer/stable/.

24. As an analogy, imagine being part of a large crowd of people. When you wanted to find something, you would ask those five people nearest you if they had it. They would then ask those around them, most of whom were not hearing directly from you, if they had it. This request would be passed along as many as seven times. If at any point your request reached someone who had it, word would be passed back to you though the same chain of people who passed your request forward.

25. This search system worked well when the network was small, but didn't scale well. As more users joined the system, the overall number of requests grew too large for the system to cope with effectively. In 2001, the search system changed to the protocol defined in the Gnutella 0.6 definition. Instead of all peers being equal, a small subset of peers that had generally better network connectivity and computing power were promoted to be "ultrapeers." Each normal peer connects to a few ultrapeers, and upon doing so tells each ultrapeer what files it has available for download. Ultrapeers connect to a larger number of other ultrapeers.

26. Under this new system, when a user wants to search, the user makes a search request in the same way as before, but instead of the request being forwarded through other peers, it is made to the few ultrapeers to which the peer is connected. These ultrapeers forward the request to their larger set of ultrapeers.

27. There are many cases in which a search for a particular file might not identify any matches even though the file exists in the network. During times of high use, network congestion

Exhibit 20

can lead to search requests going unfulfilled due to lack of capacity. Peers that contain particular files might leave the network for a while, either if the machine is shut down or the Gnutella software is stopped. Searches also cover only a portion of the network. A peer might be connected to an ultrapeer that is connected only to ultrapeers that have no information about the file requested. The search would fail in this case, though a search from another part of the network that reached the correct ultrapeers would succeed.

28. One additional type of search that LimeWire supports is a hash search. Recall that a hash is a long number computed based on all the data that makes up the file and is statistically unique to that file and which is essentially impossible to forge. A peer in possession of a file can compute the hash and then submit a search request containing that hash to search for other peers that have the identical file. Subject to the limits of search described above, the peer would then receive a list of other peers that have the bit-for-bit identical file.

C. Browsing in Gnutella

29. In addition to searching, many Gnutella clients, including LimeWire, supported a function called host browsing or simply browsing. Using this functionality, a peer that was connected to another peer, perhaps while downloading a file as a result of a search, could request a list of other files that the other peer was also making available.

30. A document Complaint Counsel has provided to me can be used to illustrate the host browsing function. This document, Exhibit CX0152 (FTC-LABMD-003755), is a screenshot of some of the files in the LimeWire sharing folder on the LabMD computer used by the company's billing manager. The screenshot includes the names of 43 (of about 950) files freely available through the LimeWire program on that computer. Materials I have reviewed show that the billing

Exhibit 20

manager used LimeWire to share music files.[5] If an outside LimeWire user searched for and found a particular music file or, for example, the “W-9 Form” file in the LimeWire sharing folder on the LabMD computer used by the billing manager, the outside user could view all the other files in the sharing folder without any further searching. As Exhibit CX0152 shows, the 1,718 File is included in the LimeWire sharing folder on the billing manager’s computer. The outside user could open and download any of the other folders in the sharing folder.

31. This feature allows a more general approach to discovering files of interest inside the Gnutella network. Users can look through the shared folders of other users that have collections of files that match their interests. If one file of some particular type is identified through search, a user might find it worthwhile to browse the other user’s files to see if anything else of interest is available.

IV. Materials Considered in Forming Opinions

32. In reaching my opinions, I have considered: Mr. Fisk’s report and materials included therein; my long experience in computer networking and digital investigations; contemporaneous security references; academic papers about p2p networks and the experiments researchers have conducted on them; and a copy of the LimeWire source code for version 4.16.6. A list of all of the materials that I considered in reaching my opinions is attached to this report as Appendix B.

33. Based on any new information that is relevant to this litigation that comes to my attention subsequent to the submission of this report through depositions or otherwise, I reserve the right to supplement my opinions as I find appropriate.

[5] See Deposition of Alison Simmons, February 5, 2014, p. 100; Deposition of John Boyle, January 28, 2014, p. 62.

Exhibit 20

V. Rebuttal to the Expert Report of Adam Fisk

34. I have reviewed the report of Adam Fisk. Complaint Counsel has asked me to provide opinions about Mr. Fisk's conclusions reached in this report concerning LimeWire and the 1,718 File. In this section I address several of Mr. Fisk's conclusions in turn.

A. Most Likely, the 1,718 File was Inadvertently Shared to the P2P Network

35. Complaint Counsel has asked me to provide an opinion responding to Mr. Fisk's discussion of how the 1,718 File was made available to the Gnutella p2p network. As discussed below, I conclude that the file's availability was likely inadvertent and the result of user error.

36. In his report on page 23, Mr. Fisk describes the steps that would be required to expose the 1,718 File on the network using LimeWire. He writes that Ms. Woodson (LabMD's billing manager):

a. "Installed LimeWire on her computer even though it clearly violated company policy

b. Actively chosen to share her My Documents folder, which LimeWire did not share by default

c. Actively saved the insuranceaging_6.05.071.pdf file in that folder."

37. These steps are essentially correct. Someone did install LimeWire, though I cannot offer an opinion as to whether doing so violated company policy. Someone did choose to share the "My Documents" folder, possibly even in face of warnings about the security risks of doing so. And somebody did place the 1,718 File in that folder where it would be shared. It seems reasonable to assume it was Ms. Woodson who did so.

38. It would be incorrect, however, to conclude from the evidence that she did so with the purposeful intent of sharing the file on the Gnutella network. Using a commonly-used directory

Exhibit 20

such as the “My Documents” folder for file sharing was then and is still a known problem and in fact appears common enough that LimeWire added a warning to notify users when this was happening. That Ms. Woodson likely placed the 1,718 File in her My Documents directory is not indicative of any particular intention to share it. That directory was a default location commonly offered by programs as a location to place files. In the absence of any evidence of her intentions, the most likely reason that LimeWire was sharing that directory and that the 1,718 File was there was simple user error.

B. Dangers of Inadvertent Sharing on P2P Networks

39. Running a p2p protocol is like advertising that anyone can come and take things from your garage. This doesn’t present problems as long as you intend for things in the garage to be taken, but should you leave sensitive or valuable things in your garage, this can go quite wrong. The garage in this analogy is the folder of shared items on the computer. Another danger is that the user will specify the wrong folder to share, in effect allowing anyone to take things from perhaps the whole house instead of just the garage.

40. The security risks of p2p software, including inadvertent file sharing, have been known since the early 2000s. While we don’t have access to a time machine to revisit that time, it is possible to find contemporaneous documents that describe the risk. Many examples come from the SANS Reading Room. SANS is the System Administration, Networking, and Security Institute. It is a well-respected organization dedicated to training systems administrators who operate and maintain computer systems and networks in the practice of security. SANS materials are a prime resource for information technology practitioners. Its advanced students produce papers on security topics which are then made publicly available on the SANS website. Looking

Exhibit 20

back at papers shows many that described the risks of p2p software at the time. I quote a few below.

41. Once such paper, titled “Peer-to-Peer File-Sharing Networks: Security Risks” was written by William Couch and contributed to the SANS reading room in 2002.[6] He wrote:

> “Another real danger of P2P networks is that, although theoretically the user controls what subdirectories he/she makes available to peer users, sometimes more subdirectories are shared than is known or intended.” (p. 6).
>
> And:
>
> “Therefore, it is up to users, and security administrators, to be aware of the risks implicit in this wide-open architecture. The safest course of action is to not use, or allow, P2P file-sharing software.” (p. 11)

42. About the same time, another student, Kelvin Choi, contributed a paper titled “Security Implications of “Peer-To-Peer” Software” dated July, 2004.[7] In it, he writes:

> “File sharing applications such as this present multiple exposure opportunities for the enterprise. Issues of intellectual property are paramount. Companies bear some measure of liability for employees trading and storing copyrighted works in the office. Equally distressing is the opportunity for unintentionally sharing proprietary or delicate information through carelessly or improperly configured clients. Allowing documents to be shared without explicit permissions is an easy mistake for the unwary user, and users have been known to unintentionally share entire disc volumes. This “information leakage” could be the most expensive security issue faced by the enterprise, as it has can have [sic] the greatest legal liability. This is exacerbated when employees install and configure file-sharing software outside a defined security process and infrastructure.” (p. 4)

43. Similarly, Lucas Ayers wrote in a paper titled “Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications” which is dated December 20, 2003:[8]

> “It appears most of the sharing of personal files is due to user error – where a user mistakenly shares documents they didn’t mean to. While this is not a true technical issue like firewall rule sets or router access lists, it is very much a Security issue. Informing users about security and making everyone aware of the

[6] See https://www.sans.org/reading-room/whitepapers/policyissues/peer-to-peer-file-sharing-networks-security-risks-510.
[7] See http://www.giac.org/paper/gsec/2016/security-implications-peer-to-peer-software/103490.
[8] See http://www.giac.org/paper/gsec/3519/security-ramifications-peer-peer-p2p-file-sharing-applications/105733.

Exhibit 20

> consequences of their actions, is one of the most imports tasks any security office has.
>
> There are also issues with the wizards and setup programs of some of these file sharing applications used during installation. The wizards will ask the user if they want to search for the location of typical files people share. If you happen to have a bunch of music files located in your "My Documents" folder (this is a typical location people have personal files on their computers), the setup program will share that whole folder with the rest of the P2P network. Not just the music you meant to share, but everything in that folder!" (p.13)

44. Again in 2003, Stephen Farquhar contributed a paper, titled "Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment," in which he writes:[9]

> "Sharing the File Server in one easy step - Astute users will selectively share files, but many users accept application defaults or blindly tick the first checkbox they see. This can result in the entire contents of their hard drive being shared or worse, all drives including network drives to be shared. Hence, unwittingly exposing the contents of the corporate file server to the public becomes a minor task." (p. 7)

as well as:

> "The task of preventing the use of P2P applications in the corporate environment is a subset of the task of preventing any unauthorised software usage and starts with policy, followed by a variety of techniques to form multi-layered defences." (p. 14)

45. These early works show that there was an awareness of computer security professionals that p2p networks provided a large risk, in no small part because a user could allow sharing of proprietary or confidential corporate documents.

46. This knowledge was not confined to SANS students. By 2005, there were warnings available through the US Computer Emergency Readiness Team about p2p networks.[10] It is possible to see a snapshot of a web page from that period through the Internet Archive Wayback Machine, which has been taking and preserving occasional snapshots of sites around the Internet

[9] See http://www.giac.org/paper/gsec/3123/peer-to-peer-p2p-file-sharing-applications-threat-corporate-environment/103882.

[10] The United States Computer Emergency Readiness Team (US-CERT) is a government agency leading efforts to "improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a dynamic and complex environment." See http://www.us-cert.gov/about-us.

Exhibit 20

over a long period of time. One such web page is at:

http://web.archive.org/web/20051127091241/http://www.us-cert.gov/cas/tips/ST05-007.html.

This page, captured in November 2005, but marked as updated in June 2005 reads in part:

> "**Exposure of sensitive or personal information** - By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft (see Protecting Your Privacy and Avoiding Social Engineering and Phishing Attacks for more information)."

47. By 2005, various organizations had warned about the risk of inadvertent file sharing through p2p programs, and by 2006, concern about p2p networks and defending against security problems they had caused had reached the state of best practice. As seen in the document "Security Best Practices", written by Dr. Eric Cole (a security consultant and SANS instructor):[11]

> "The most important security practice, that which all other security controls and protections are based on, is the creation and enforcement of security policies. Every organization must have an overall policy that establishes the direction of the organization and its security mission as well as roles and responsibilities. There can also be system specific rules to address the policies for individual systems and data. Most importantly, the appropriate use of computing resources must be addressed. In addition, policies can address a number of security controls from passwords and backups, to proprietary information. There should be clear procedures and processes to follow for each policy. These policies should be included in the employee handbook and posted on a readily accessible intranet site.
>
> The organization's security policies should address applications, services and activities that are prohibited. These can include, among others, viewing inappropriate material, spam, **peer-to-peer file sharing**, instant messaging, unauthorized wireless devices and the use of unencrypted remote connections such as Telnet and FTP. Appropriate use policies should outline users' roles and responsibilities with regard to security. They should provide the user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If an organization identifies specific actions that could

[11] See http://www.securityhaven.com/docs/Security_Best_Practices.pdf.

Exhibit 20

> result in punitive or disciplinary actions against an employee, these actions and ways to avoid them should be clearly explained in the policy." (p. 2, emphasis added)

48. The fact that inadvertent sharing of sensitive documents was a concern and needed to be prevented by specific policy, procedure, and training was well known among information technology practitioners by 2006. By 2005, other organizations were warning about risks presented by p2p programs to more general audiences.[12]

49. For the reasons set out above, p2p programs presented a well-known and significant risk that files would be inadvertently shared. Because the LimeWire sharing folder on the LabMD computer used by the billing manager included hundreds of files, including music files and .pdf files, it is likely that the 1,718 File was inadvertently included in the sharing folder.[13]

C. Searching Using LimeWire/Gnutella Functionality

50. Complaint Counsel has asked for my opinion about Mr. Fisk's conclusion about the ways by which the 1,718 File could have been found and copied from the LabMD computer of Rosalind Woodson, LabMD's billing manager, using LimeWire. As I explain below, I believe there are other ways the 1,718 File could be found besides the exact file name search Mr. Fisk identifies.

51. Mr. Fisk makes the point that it would be difficult for a searcher to create a search that would find the file named "insuranceaging_6.05.071.pdf" on pages 11-13 of his report. He states that the searcher would have to enter either the term "insuranceageing" or "6.05.071" in order to find the file.

52. Mr. Fisk concludes that "it is extremely unlikely that any *typical* user of the Gnutella network, including highly sophisticated users, would ever have found the

[12] See, e.g., http://www ftc.gov/news-events/press-releases/2005/06/ftc-issues-report-peer-peer-file-sharing.

[13] Mr. Fisk presents no evidence to support his alternative hypothesis that the file was shared by email or portable media, which I discuss in Section D, below.

Exhibit 20

"insuranceaging_6.05.071.pdf" file in question using search alone."[14] He also concludes that "only extremely sophisticated and custom-designed software would ever be configured in this fashion," meaning in a way suitable for locating the 1,718 File.[15]

53. Mr. Fisk reaches his conclusion in part based on an unreasonable assumption about how the file could be found, ignoring a variety of other methods that would account for its eventual exposure through LimeWire.

54. His conclusion addresses only one very narrow possibility of how the file might have been discovered through the Gnutella network, which is searching for it based on its exact name.[16] This conclusion is almost certainly incorrect as there is at least one search method that could return the file without using either of the two file name terms Mr. Fisk identifies.

55. More importantly, he does not conclude that the 1,718 File was not downloaded using the LimeWire program that was indisputably sharing the file. His report instead hints at a number of ways that it could have happened, and he addresses and rules out none of them.[17] There are viable ways that the file could have been found and copied from the LabMD system and I describe below three simple, relatively unsophisticated methods, other than using the two file name terms Mr. Fisk identifies, by which the 1,718 File could have been retrieved through LimeWire.

i. Browsing

56. LimeWire contains functionality that allows any user of the network to connect directly to another computer running LimeWire. Once connected, the user can see all files that are

[14] Fisk Report, p. 16.
[15] Fisk Report, p. 24.
[16] Fisk Report, p. 13.
[17] Fisk Report, pp. 24-25.

Exhibit 20

available for download. This information is most often presented as a list that the user can scroll through, and should the user choose to, he or she can click on any file and download it directly.

57. The simplest way this "browse host" functionality might have been used to download the 1,718 File is for a user to have received a search hit for some other file that was present on the LabMD computer running LimeWire, and then chosen to use the "browse host" function to examine and download other files from the computer. My understanding is that Ms. Woodson was using LimeWire to download and share popular music that could result in many search hits. This could easily have led to the 1,718 File being downloaded through browse host.

58. In addition, the shared folders on Ms. Woodson's computer contained other files that might have drawn the interest of potential thieves and could have been found through the basic search. For example, there was a file named "W-9 Form" being shared.[18] A person who was interested in identity theft might have been searching on that term to find addresses and Social Security numbers. The browse host function could then be used to view and download the 1,718 File that was contained in the same shared folders.

59. While it may be unlikely that any random user would choose to download the 1,718 File, this low probability must be balanced against the enormous number of users on the Gnutella system. An analogy is the Powerball lottery. The chance of any one ticket winning is low, but given that so many people buy tickets the lottery is won relatively frequently.

60. Mr. Fisk, on page 15 of his report, states:

> "At any one time on the LimeWire network there would be approximately 2 to 5 million users online."

[18] Citizens use the Internal Revenue Service's W-9 Form to request a taxpayer identification number. In completing the form, citizens enter, among other things, their names, addresses, and Social Security numbers. Internal Revenue Service, "Request for Taxpayer Identification Number and Certification" (November 2005), *available at* http://dese mo.gov/se/documents/se-fs-w9.pdf.

Exhibit 20

61. Over an extended period of time, such as weeks or months, even a 1 in 1,000,000 chance of someone downloading the 1,718 File would therefore result in it being downloaded many times. It takes only one such download to allow the information to be released.

62. Mr. Fisk also goes into detail describing the LabMD firewall's operation, but also implies that the firewall would not have prevented the "browse host" feature from being used when he states on page 16:

> "In order to download the files of a browse host either the Downloader or the Uploader must not be behind a firewall."

63. While the LabMD computer was behind a firewall, any computer that itself was not behind a firewall could therefore have used the browse host function to download the 1,718 File.

ii. Searches for Misconfigured P2P Peers

64. Above, I discussed the possibility that a random user found and downloaded the 1,718 File from the LabMD computer through LimeWire using the "browse host" function. There is a more deliberate way that the file could have been found and downloaded.

65. The Internet, being a public network, is sometimes used by people who might have fraudulent or malicious intent, including those looking for sensitive documents that p2p users did not intend to share. One opportunity for them to get documents is to identify and exploit misconfigured p2p nodes that are likely to expose sensitive information, then to download and make use of that information. Notably, these actors do not need to have any information about the names of the files they hope to find. Instead, they gather open information about common files that are placed in particular directories when installed. For example, they can search for particular operating system files that appear under the directory C:\windows, or common files installed by applications that are placed in the "My Documents" folder. A badly mis-configured

Exhibit 20

Windows XP node that was sharing its C: drive would be easily identifiable by searching for a file named Zapotec.bmp, which is a default file included in that version of Windows.

66. Finding one of these files would signal a high probability that the LimeWire program on a computer was misconfigured and was currently exposing files in the directory where files like the 1,718 File are normally found. For example, a file known to be installed in “My Documents” that was found as a result of a search would indicate that that computer was exposing the “My Documents” folder, which is likely to contain a large number of files of various types. The person would then connect to that computer and use the “browse host” functionality to download and examine potentially interesting files that were exposed.

67. The LabMD computer, which was running LimeWire, would have been vulnerable to being found in this manner. Unfortunately, LabMD produced incomplete information about which files were being shared so it is difficult to identify which files might have been the lure to attract someone who was actively seeking misconfigured peers. Nevertheless, the fact that the information was being made publicly available on a network known to be used by malicious actors means that there is a reasonable possibility the file could have been discovered in this manner.

iii. File Extension Search

68. As noted above, Mr. Fisk writes extensively to make the case that it would be difficult for a searcher to find the 1,718 File using its filename.[19]

69. I believe he is mistaken, and there is one simple and direct search that would return that file, which is to search on the portion of the filename he neglects – the file extension “pdf.”

[19] Fisk Report, pp. 13-16, 23.

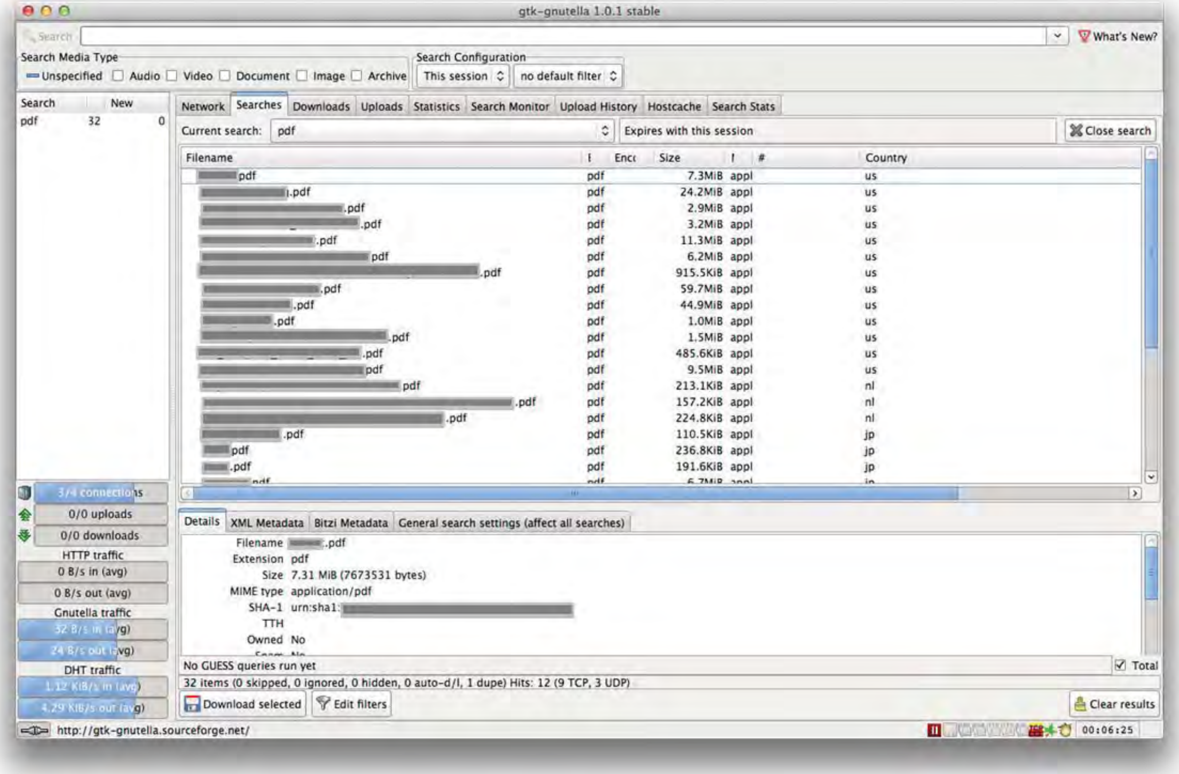
Exhibit 20

70. The file extension "pdf" indicates that the file is formatted as an Adobe Portable Document Format (PDF) file. This format is commonly used for documents that contain text and images, but which are not intended to be edited. It is very commonly used in academic and business environments for distributing documents. I have also encountered entire books being formatted and shared as PDF files.

71. Gnutella users who are searching the network might then choose to search for PDF if they had interest in those types of documents. Such a search would easily return the 1,718 File. To demonstrate that this is possible and easy to do, I performed searches with the current Gnutella network using the "gtk-gnutella" program and verified that a search using the term "pdf" returns search results that consist of PDF files, the bulk of which contain the string "pdf" only in the file extension. The image below shows the results of such a search using the gtk-gnutella program, version 1.01 available from http://gtk-gnutella.sourceforge.net/ and the files it returned.[20]

[20] Files names except for extensions have been redacted in the image.

Exhibit 20



Search Media Type: ▬ Unspecified □ Audio □ Video □ Document □ Image □ Archive

Search Configuration: This session | no default filter

Search	New	
pdf	32	0

Current search: pdf

Expires with this session

Filename	I	Encc	Size	I	#	Country
[redacted]pdf	pdf		7.3MiB	appl		us
[redacted].pdf	pdf		24.2MiB	appl		us
[redacted].pdf	pdf		2.9MiB	appl		us
[redacted].pdf	pdf		3.2MiB	appl		us
[redacted].pdf	pdf		11.3MiB	appl		us
[redacted]pdf	pdf		6.2MiB	appl		us
[redacted].pdf	pdf		915.5KiB	appl		us
[redacted].pdf	pdf		59.7MiB	appl		us
[redacted].pdf	pdf		44.9MiB	appl		us
[redacted].pdf	pdf		1.0MiB	appl		us
[redacted].pdf	pdf		1.5MiB	appl		us
[redacted].pdf	pdf		485.6KiB	appl		us
[redacted]pdf	pdf		9.5MiB	appl		us
[redacted]pdf	pdf		213.1KiB	appl		nl
[redacted].pdf	pdf		157.2KiB	appl		nl
[redacted].pdf	pdf		224.8KiB	appl		nl
[redacted].pdf	pdf		110.5KiB	appl		jp
[redacted]pdf	pdf		236.8KiB	appl		jp
[redacted].pdf	pdf		191.6KiB	appl		jp
[redacted]pdf	pdf		6.7MiB	appl		jp

Filename [redacted].pdf
Extension pdf
Size 7.31 MiB (7673531 bytes)
MIME type application/pdf
SHA-1 urn:sha1:[redacted]
TTH
Owned No

No GUESS queries run yet ☑ Total

32 items (0 skipped, 0 ignored, 0 hidden, 0 auto-d/l, 1 dupe) Hits: 12 (9 TCP, 3 UDP)

72. The question then becomes "Did LimeWire support this type of search during the relevant period?" Unfortunately, LimeWire was ordered closed, and at that point we lost full access to the site containing the source code and documentation.[21] We do, however, have some remnants of the LimeWire site as recorded by the Internet Archive Wayback Machine.

73. Searching using the Wayback Machine allowed me to retrieve a copy of the LimeWire source code for version 4.16.6, which was similar to the version that was running on the LabMD computer Rosalind Woodson used.[22] It was the closest version to the version 4.16.7 on the LabMD computer that the Wayback Machine had archived, and is very close to the code running

[21] *Arista Records, LLC v. Lime Group LLC*, 715 F. Supp. 2d 481, 96 U.S.P.Q 2d 1437 (S.D.N.Y 2010).

[22] I downloaded this code from the URL: http://web.archive.org/web/20081203173114/http://www.limewire.org/limewire.zip.

Exhibit 20

on the LabMD computer, judging from the version number. I examined the code of the program to determine if file extensions, such as ".pdf" were excluded when searching with LimeWire.

74. I found no such code. Instead, I found code that supports the theory that LimeWire allowed searches by file extension and then returned files containing that file extension. In the file from the source code distribution named GreedyQueryFilter.java, there is code to limit searches that would be excessively burdensome on the Gnutella network. The code in question is named `isVeryGeneralSearch`, lines 43-65. I will spare quoting the code in detail, but the comment describing the code is accurate as to its functionality and reads:

a. "Search through a query string and see if matches a very general search such as "*.*", "*.mp3", or "*.mpg" and check for uppercase also"

75. This shows that the code blocked searches based on the file extensions ".mp3" and ".mpg", which are for music and audio files and movie files, respectively. This strongly implies that searches based on file extensions were possible, and that those searches for PDF files were not blocked. Assuming the implication is correct, file extension searches were possible in LimeWire and would have returned the 1,718 File.

76. Again, this indicates that users who were searching for the types of documents that are commonly found in businesses, such as Microsoft Office documents and PDF files, could have easily found the 1,718 File using search without using any more specific terms.

D. Searching Outside the Gnutella Mechanism

77. Complaint Counsel has asked me to provide an opinion about Mr. Fisk's conclusion that only "sophisticated organizations capable of deploying the financial and ultimately technical resources required" to write and use custom search software to crawl p2p networks could locate the 1,718 File. These programs would be written to make use of the protocol mechanisms to

Exhibit 20

traverse the network to catalog its participants and the names of content they were sharing instead of downloading code. As I explain below, creating such software is not limited to “sophisticated organizations.”

78. Mr. Fisk first makes the incorrect assumption that the 1,718 File had to have been found by searching exactly for either of the two file name terms he identifies.[23] As discussed above, this assumption is incorrect as it was entirely possible for the file to be located without searching by either of file name terms Mr. Fisk identifies. Following from this first incorrect assumption, he then states that the only way for this document to have been located on the Gnutella network was through custom search software, implying that this software must have used the “browse host” function to search through files on all hosts.[24] He then uses the assumption of custom software to state that only a “sophisticated” organization with large financial and technical resources could write such code, and that such code indicates knowledge no normal network user would have.[25] Finally, he suggests that the other copies of the 1,718 File located on LabMD’s network were therefore found by and later shared by one of these organizations.[26]

79. This chain of logic is almost entirely incorrect. Custom search software using the “browse host” function is not difficult to create, as most of the code needed already exists and is freely available. It would require little specialized knowledge of the protocol as the code available already encodes protocol knowledge. Because the code is readily available, almost anyone with the necessary undergraduate-level programming experience could create it, and a brief search finds evidence that this has happened. The organizations that Mr. Fisk suggests might have created such software also have incentives not to share what they might find, and it is

[23] Fisk Report, p. 13.
[24] Fisk Report, p. 24.
[25] Fisk Report, pp. 24-25.
[26] Fisk Report, pp. 24-25.

Exhibit 20

unlikely, had they downloaded any files from the network, that they would have then shared them.

80. Mr. Fisk's argument makes the following points:

a. Implicitly, he assumes that the file can only be found by searching for it using its filename.

b. He then claims that no ordinary user could have found the 1,718 File using normal search.

c. As search must have been used, but normal search would not have worked, then the person who found it must have written their own search.

d. This search must have used the "nuances" of the "browse host" functionality.

e. No ordinary user could or would write their own search this way; they would not have the technological resources to do so.

f. Therefore, it must have been an organization like Tiversa, the FBI, Big Champagne, or the RIAA.

g. Because the file was later found at multiple IP addresses online, it is possible that it was then being shared by the organizations above who had created their own search software.

81. I have addressed points a and b in Section A above. There is no need for the file to have been found only by searching for its filename. It could have been randomly browsed, found as part of a search for misconfigured peers, or found by searching for the term "pdf," as I explained above. Below I address his custom search argument (points c, d, e, and f).

Exhibit 20

i. The Challenge of Creating Custom Search Software

82. Though it is clear that writing a custom search was not necessary, I would like to address the points c, d, e and f regarding writing custom software. Mr. Fisk is incorrect in most particulars. Writing such software is not challenging, as most of the code exists and embeds the necessary knowledge of the protocol. It might take only someone with an undergraduate computer science degree and basic networking knowledge, and there is evidence that this has happened.

83. First, Mr. Fisk is not very precise in defining what constitutes an "ordinary user." There are distinctions that need to be made in discussing what a *user* of p2p software can do with the software, and what a *developer* who is extending p2p software can make the software do in accordance with the Gnutella protocol. In the first case, an "ordinary user" would be one who uses an existing p2p software client, like LimeWire. They would be limited to the functionality that was built into the software by the developers. In LimeWire, these are things like search, download, and browsing a host where you have located a file.

84. The developer of the software, however, has access to all the functionality that the Gnutella protocol provides. This is more functionality than is commonly built into the software. The reason is that the protocol provides a variety of possible services which are generally used in one way, say to provide normal search and download services, but which can be recombined in a different way, say to create a browse-based search, in a way that does not violate the operation of the protocol. In the example of a browse-based search, the developer would choose to combine the portion of the protocol that does peer-discovery with the portion of the protocol that allows host browsing to extract the information of what files are in the network. The developer could then create his or her own index and search across that. Such activity is normal or ordinary from the point of view of the other participants of the protocol.

Exhibit 20

85. Second, Mr. Fisk implies that creation of this software is something that is out of reach of the average developer. He states (page 24):

> "The vital point is that only extremely sophisticated and custom-designed software would ever be configured in this fashion"

and (page 24, again):

> "In order to find the 1,718 File someone would have to understand the nuances of the browse host message and would have had to have written custom software to take advantage of that knowledge."

86. This implication is not the case. A programmer who wanted to create software that took advantage of the Gnutella network can draw on a publically available and well-documented code base that would provide most of the functionality needed.

87. As I am fond of explaining to my programming classes, programmers are lazy – but they are lazy in a good way, which means doing as little work as possible to achieve whatever programming goal they are trying to reach. This often is demonstrated by the reuse of existing code. It is generally faster and easier to find code that does what you want than it is to write it yourself. In fact, code reuse is highly encouraged in the computer science community, and languages like Java include a concept called "classes" which allow ease of code reuse.

88. To support code reuse, there are often practices to help generate documentation as code is written, so that other programmers can more easily understand the existing code. Java uses a system called "javadocs" that allows programmers to annotate their code, and then to later use the annotations as the input to a program that converts them to readable documentation.

89. LimeWire itself is written in Java, and uses javadocs to create documentation. There are other Gnutella clients available as well, and a programmer who wanted to extend the Gnutella

Exhibit 20

functionality could download the source code of the programs and use that as a basis for this work. This would greatly increase the ease and speed of developing code that works with the Gnutella protocol.

90. Using existing code for Gnutella removes the need for programmers to completely understand all aspects of the Gnutella protocol, as the Java language classes already written encapsulate the knowledge of the original programmer. Others can then use the interface in the class to interact with Gnutella without needing full knowledge of how the protocol works. This removes the need for other programmers to understand all the details of the protocol.

91. Most networking code is written in this way. Networking code is divided into a series of components, known as the "networking stack." Each layer of the stack provides an interface that enables functionality without requiring deep protocol knowledge, so reusing Gnutella code would be a natural extension of this approach.

92. To see if there was evidence to support the idea that large-scale cataloging of files that were available on Gnutella through the browse host function was not as challenging as Mr. Fisk indicates, I did a brief search of academic literature through Google Scholar. I found several academic papers describing the results of crawling the Gnutella network. One in particular described developing a crawler that could access all the ultrapeers in the network in under 10 minutes in 2005. This work was titled "Capturing Accurate Snapshots of the Gnutella Network" by Daniel Stutzbach and Reza Rejaie, and appeared in 2005 at a prestigious peer-review networking conference.

93. A later publication using the same crawler also documented the files that were available on the Gnutella network. In this case, they modified the crawler above to also issue "browse host" requests to catalog the contents of the network. This work appeared in another prestigious

Exhibit 20

peer-reviewed conference in 2006 and was titled "Characterizing Files in the Modern Gnutella Network: A Measurement Study" by Shanyu Zhao, Daniel Stutzbach, and Reza Rejaie.

94. Looking at the authors list, it appears that Shanyu Zhao and Daniel Stutzbach were graduate students, and Reza Rejaie was a professor at the time. This small team, with no acknowledged funding, was able to develop a high-speed crawler that used the Gnutella browse host extension to catalog the network. This is one paper of many that describe crawling the Gnutella network.

95. I will also note that crawling Gnutella is a common enough activity that it has its own Wikipedia page at http://en.wikipedia.org/wiki/Gnutella_crawler.

96. This indicates that creating a crawler is not as difficult as Mr. Fisk implies, and certainly isn't the sole province of a large and well-funded organization.

ii. Crawling versus Sharing

97. In point g of his argument above, after suggesting the 1,718 File must have been found by a crawler from a large organization such as the FBI, Big Champagne, Tiversa, or the RIAA, Mr. Fisk then suggests that the other copies of the files that are available on the network might come from these crawlers.

98. Mr. Fisk is incorrect in this assertion because the organizations above, were they to download files, would have no motivation to then share them.

99. Instead, it is possible to download files without sharing them again on the network. Even an ordinary LimeWire user could prevent re-sharing files by separating the download folder from the shared folder.

Exhibit 20

E. Other Avenues of Information Disclosure

100. Complaint Counsel also asked me to provide an opinion about Mr. Fisk's conclusions as to other methods by which the 1,718 File could have been downloaded or disclosed. In this section, I discuss his conclusions about thumb drives and email.

101. After apparently reaching the erroneous conclusion that the installation and use of LimeWire could not have been a possible source of the 1,718 File leaving the LabMD network, Mr. Fisk attempts to propose some other mechanisms by which the file could have left the network. On page 25, he suggests that the file could have been emailed out of the organization or placed on a thumb drive and removed. Unfortunately, Mr. Fisk points to no evidence to support that either of these actions occurred. By contrast, there is ample evidence that LimeWire was in use.

102. One of my areas of research and experience is in the area of digital forensics, which is the investigation of misuse or crime that might have left evidence on digital devices. I have had extensive training in commercial forensics tools and operation and am well aware of the types of evidence that are left behind on a computer system when data is either copied to a USB stick or sent by email. It is frequently, though not always, possible to recover artifacts relating to these transfers. For a USB stick, there is evidence of what USB sticks were inserted into the system and, often, what files were copied to them. For email, it is often possible to recover the sent email from the outgoing messages folder or from backups from the mail server to verify what was sent.

103. Unfortunately, it is not possible to conduct such an examination in this case as the system that was being used was not properly preserved for investigation. Doing so would have required making a copy of the hard drive in its entirety and keeping the drive and copy unaltered. The

Exhibit 20

evidence is that this was not done.[27] As opposed to the lack of evidence for any of Mr. Fisk's alternate scenarios, there is substantial evidence that LimeWire was the source of the disclosure. We know that:

a. The computer at LabMD was running LimeWire and was sharing the 1,718 File.

b. People who download files from Gnutella most frequently store them in their own shared directory, which in turn makes them available to the file-sharing network.

c. The 1,718 File was found being shared on the Gnutella network. To appear there, it had to be placed in a folder on a computer that was being shared.

104. The most likely conclusion, then, is that the file was available and being shared via the LabMD computer. Others downloaded it, and as is common, stored it in their shared folder. It was then available for others to discover, and it was then found being shared elsewhere.

105. Overall, Mr. Fisk provides no evidence that supports his suggestion that the file was taken out of the network by some means other than through LimeWire.

VI. Conclusion

106. Based on my experience described in Section II, my review of the material described in Section IV, and the specific opinions presented in Section V, my overall conclusion is that Mr. Fisk is mistaken in his conclusion that the 1,718 File could only have been located by a sophisticated organization with considerable resources. In addition, his theory that the file was disclosed through a thumb drive or by e-mail is unsupported by any evidence. Overall, I conclude that the 1,718 File was likely inadvertently disclosed by LabMD's billing manager when she used LimeWire on her LabMD computer.

[27] Mr. Daugherty testified that the hard drive from the LabMD computer used by the billing manager and a copy of the hard drive were rendered unusable by a security consultant LabMD engaged. See Deposition of Michael Daugherty, March 4, 2014, pp. 203-07.

Exhibit 20

Dated: April 11, 2014

Clay Shields, Ph.D.

Exhibit 20

APPENDIX A

Exhibit 20

APPENDIX A

Clay Shields

Department of Computer Science
Georgetown University
Washington, DC, 20057
clay@cs.georgetown.edu
(202) 687-2004

Academic Experience

Professor, Georgetown University, August 2011 - Present
Associate Professor, Georgetown University, August 2005 - August 2011
Assistant Professor, Georgetown University, August 2001 - August 2005

One of the top teachers in the Computer Science department as rated by students. Nominated twice for the Dean's Teaching Award. Teaching classes in programming, networks, operating systems, and computer and network security. Conducting research in computer and network forensics, and on anonymous communication.

Director, Georgetown Institute for Information Assurance, 2002 - Present

As Director, initiated and led the effort that resulted in Georgetown University being declared an NSA Center of Excellence in Information Assurance. This award covers the whole university, and makes Georgetown eligible for scholarships and development funding from the NSA. Earning this designation first required showing that Georgetown's Information Assurance curriculum met the Information Assurance Courseware Evaluation standards. Afterwards, completed an accreditation process requiring coordination between information assurance faculty across schools within Georgetown. Next formed a partnership with the National Defense University to bring externally-supported graduate students into the Computer Science Master's degree program.

Assistant Professor, Purdue University, August 1999 - July 2001

Assistant professor in computer science, and associated with CERIAS, the Center for Education and Research in Information Assurance and Security. Conducted research into network forensics and anonymity. Taught courses in network security, information assurance and operating systems.

Instructor, Central Texas College, 1992 - 1993

Instructed fourteen distance-learning college level courses covering a variety of subjects in the Arts and Sciences for U.S. Army soldiers stationed in the Sinai. Rated as "excellent" on student evaluations.

Education

University of California at Santa Cruz, 1994 - 1999

PhD in Computer Engineering, June, 1999.
Advisor: J.J. Garcia-Luna-Aceves.
Dissertation: Secure Hierarchical Multicast Routing and Multicast Internet Anonymity.

Masters in Computer Engineering, June, 1996.
Master's Thesis: Ordered Core Based Trees.

University of Maryland, 1993 - 1994

Graduate-level course work in Computer Science.

University of Virginia, 1984 - 1989

Bachelor of Science, Electrical Engineering.

Exhibit 20

Professional Experience

Principal, Computer Litigation Resources, LLC, May 2005 - August 2010
Principal of consulting business for conducting forensic computer examinations and providing expert testimony on the results. Prepared and delivered forensic courses for Ernst & Young, LLP, internal training. Qualified by the 19th Judicial Circuit of Virginia as an expert witness on computer forensics.

Staff Scientist, Cenus Technologies, July 2000 - September 2000

Consulting on network security issues for Internet start-up.

Security Coordinator, University of California at Santa Cruz, 1997 - 1998

Responsible for conducting vulnerability testing, for monitoring of campus networks, and for response to security breaches. Conducted short and long-term planning for campus security systems, including investigation and testing of firewall and one-time password systems, and testing of campus certificate server system.

Infantry Platoon Leader, 101st Airborne Division, U.S. Army, 1990 - 1993

Platoon Leader of Rifle and Anti-Armor Infantry Platoons. Responsible for leadership of a 40 soldier platoon during tactical employment; planning and execution of safe, effective training; and accountability and maintenance of over one million dollars of equipment. Led platoon during six month deployment to the Sinai as part of the MFO peacekeeping force, and received Army Achievement medal for exceptional performance in that position.

Expert Witness Experience

Intellectual Property	
Consulting Witness, Plaintiff	Intellectual Ventures I LLC and Intellectual Ventures II LLC v. Capital One Financial Corporation, Capital One Bank (USA) and Capital One, N.A.,Civil Action No. 1:13cv740-AJT/TRJ, Eastern District of Virginia
Consulting Witness, Defendant	Droplets, Inc. v. Facebook, Inc., Civil Action No. 2:11-CV-392, Eastern District of Texas
Testifying Witness, Plaintiff	Creative Kingoms, LLC. v. Nintendo Co., Ltd., Case No. 337-TA-770, ITC.
Consulting Witness, Plaintiff	Juniper Networks Inc. v. GraphOn Corp., Case No. 1:09-cv-00287, Eastern District of Virginia
Computer Forensics	
Written report	Cause No F-2569-B, 93rd Judicial District Court, Hidalgo County, TX, May 2013
Testifying Witness, Plaintiff	Facility Solutions Group v. ISM Services, Inc. Fairfax County, VA, June, 2005
Consulting Witness, Plaintiff	FTC v. D Squared Solutions, AMD 03 CV3108 (pro bono)

Scholarship

Journal Articles

A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach. **"Accountable Wiretapping, Journal of Computer Security"**, to appear in Journal of Computer Security.
M. Liberatore, B. N. Levine, C. Shields and B. Lynn. **"Efficient Tagging of Remote Peers During Child Pornography Investigations"**, *Transactions on Dependable and Secure Computing, January, 2014.*

S. Cabuk, C. Brodley, and C. Shields. **"IP Covert Channel Detection"**, *ACM Transactions on Information and System Security (TISSEC)* Vol. 12, Num. 22, April 2009.

M. Wright, M. Adler, B.N. Levine, and C. Shields. **"Passive-Logging Attacks Against Anonymous Communications Systems"**, *ACM Transactions on Information and System Security (TISSEC)* Vol. 11, Num. 2, March 2008.

K. Sanzgiri, B. Dahill, D. LaFlamme, B. N. Levine, C. Shields, and E. Belding-Royer, **"An Authenticated Routing Protocol for Secure Ad hoc Networks"**, *IEEE Journal on Selected Areas in Communications: Special Issue on Wireless Ad Hoc Networks.* Vol. 23, Num. 3, March, 2005.

Exhibit 20

B. Carrier and C. Shields, **"The Session Token Protocol for Forensics and Traceback"**, *ACM Transactions on Information and System Security (TISSEC).* Vol. 7 , Num. 3, August 2004.

F. Buchholz and C. Shields, **"Providing Process Origin Information to Aid in Computer Forensic Investigations"**, *Journal of Computer Security*, Vol. 12, Num 5., 2004

M. Wright, M. Adler, B. N. Levine, and C. Shields, **"The Predecessor Attack: An Analysis of a Threat to Anonymous Communication Systems"**, *ACM Transactions on Information and System Security (TISSEC).* Vol. 7 , Num. 4, November 2004.

B.N. Levine and C. Shields. **"Hordes - A Multicast Based Protocol for Anonymity"**, Journal of Computer Security, Vol. 10, Num. 3, 2002, pp. 213-240, by invitation.

C. Shields and J.J. Garcia-Luna-Aceves,**"A Protocol for Hierarchical Multicast Routing"**, *Computer Communications*, Vol:23. Issue: 7, March 13, 2000, pages 628-641.

Patents

Automated Forensic Document Signatures, US Patent US 8,438,174 B2. C. Shields, M. Maloof, and O. Frieder.

Automated Forensic Document Signatures, US Patent 8,312,023. C. Shields, M. Maloof, and O. Frieder.

Automated Forensic Document Signatures, US Patent 8,280,905. C. Shields, M. Maloof, and O. Frieder.

Book Chapters

C. Shields. **"An Introduction to Information Assurance."** Machine Learning and Data Mining for Computer Security. Ed. Marcus A. Maloof. London: Springer, 2005.

Conference Papers

A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach. **'Accountable Wiretapping -or- I Know They Can Hear You Now"**. *Network and Distributed System Security Symposium (NDSS)*, February 2012.

R. Walls, B.N. Levine, M. Libertore, C. Shields **"Effective Digital Forensics Research is Investigator-Centric"**, *6th USENIX Workshop on Hot Topics in Security (HotSec)*, August, 2011

C. Shields, O. Frieder, M. Maloof. **"A System for the Proactive, Continuous, and Efficient Collection of Digital Forensic Evidence"**, *Proceedings of the Digital Forensics Research Conference (DFRWS)*, August, 2011.

M. Libertore, B.N. Levine, C. Shields. **"Strengthening Forensic Investigations of Child Pornography on P2P Networks"**, *Proceedings of the 6th International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, November, 2010.

M. Liberatore, R. Erdely, T. Kerle B. Levine and C. Shields. **"Forensic Investigation of Peer-to-Peer File Sharing Networks"**, *Proceedings of the Digital Forensics Research Conference (DFRWS), August*, 2010.

C. Shields. **"Towards Proactive Forensic Evidentiary Collection"**, *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*, January, 2010.

C. Piro, C. Shields. B. N. Levine. **"Detecting the Sybil Attack in Mobile Ad hoc Networks"**, *Proceedings of the Second International Conference on Security and Privacy in Communication Networks (SecureComm)*, Baltimore, MD, 2006.

S. Cabuk, R. M. Forte, C. Brodley, and C. Shields, **"IP Covert Timing Channels: An Initial Exploration"**, *Proceedings of the ACM Computer and Communications Security Conference (CCS)*, October, 2004.

M. Wright, M. Adler, B. N. Levine, an C. Shields, **"Defending Anonymous Communication Against Passive Logging Attacks"**, in Proceedings of the 2003 *IEEE Symposium on Security and Privacy (IEEE S&P)*, Oakland, CA, May, 2003.

B. Dahill, K. Sanzgiri, B. N. Levine, C. Shields, and E. M. Belding-Royer, **"A Secure Routing Protocol for Ad Hoc Networks"**, in Proceedings of the 2002 *IEEE International Conference on Network Protocols (ICNP)*, Paris, France, November, 2002.

B. Carrier and C. Shields, **"A Recursive Session Token Protocol for use in Computer Forensics and TCP Traceback"**, in Proceedings of the 2002 *IEEE Conference on Computer Communications (Infocom)*, New York, NY, June, 2002.

Exhibit 20

F. Buchholz and C. Shields, **"Providing Process Origin Information to Aid in Network Traceback"**, in Proceedings of the 2002 *USENIX Annual Technical Conference*, Monterey, CA, June, 2002.

M. Wright, M. Adler, B.N. Levine, and C. Shields, **"An Analysis of the Degradation of Anonymous Protocols"**, Proceedings of the ISOC *Network and Distributed System Security Symposium (NDSS)*, San Diego, CA., February 2002. *Received the Outstanding Paper Award*

V. Scarlata, B.N. Levine, and C. Shields, **"Responder Anonymity and Anonymous Peer-to-Peer File Sharing"**, in Proceedings of the. *IEEE International Conference on Network Protocols (ICNP)*, 2001, Riverside, CA., November 2001.

C. Shields and B.N. Levine, **"A Protocol for Anonymous Communication over the Internet"**, Proceedings of the 7th Annual *ACM Conference on Computer and Communications Security (CCS)*, Athens, Greece, November, 2000.

C. Shields and J.J. Garcia-Luna-Aceves, **"KHIP -A Scalable, Efficient Protocol for Secure Multicast Routing"**. In *Proceedings of ACM Special Interest Group on Data Communications (SIGCOMM)*,Boston, MA, August, 1999.

C. Shields and J.J. Garcia-Luna-Aceves,**"The HIP Protocol for Hierarchical Multicast Routing"**, In *Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, Puerto Vallarta, Mexico, June, 1998.

C. Shields and J.J. Garcia-Luna-Aceves, **"The Ordered Core Based Tree Protocol"**, In Proceedings of the *IEEE Conference on Computer Communications (Infocom)*, Kobe, Japan, April, 1997.

Workshop papers

C. Shields, **"What do we mean by Network Denial of Service?"**, Proceedings of the 2002 *IEEE Workshop on Information Assurance and Security*, West Point, N.Y., June, 2002.

S. Lee and C. Shields, **"Tracing the Source of Network Attacks: A Technical, Legal and Social Problem"**, in *Proceedings of the Second Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop*, West Point, NY., June 2001.

S. Mandujano and C. Shields, **"Confidentiality and Anonymity Analysis of On-Line Payment Protocols"**, *Computer Security Congress*, November 2000, Mexico City, Mexico.

Other articles

C. Shields, **"Ask the Experts - How can deleted computer files be retrieved at a later date?"**. *Scientific American*, March, 2004.

C. Shields, **"Ask the Experts - Why do computers crash?"**. *Scientific American*, May, 2003.

S. C. Lee and C. Shields, **"Technical, Legal, and Societal Challenges to Automated Attack Traceback"**, *IT Professional*, May/June, 2002. pp. 12-18.

Software

M. Libertore, B.N. Levine and C. Shields, **RoundUp**. RoundUp is a modified Gnutella client in use by various police forces to locate and create warrants for arrest for indviduals sharing child pronography online. In August of 2010, RoundUp was declared part of the US National Strategy for Child Exploitation Prevention and Interdiction. In addition, as of August 2010, RoundUp is being used by over 1,224 individual investigators and 58 Internet Crimes Against Children Task Forces. As of that date, they have used RoundUp to serve 1,258 search warrents that have so far resulted in 567 arrests. These numbers are a lower bound based on self-reporting.

C. Shields and L. Neubauer, `sdtext` creates portable text-based similarity digests that can identify similar files despite differences in format.

Tutorials

C. Shields and B.N. Levine,**"An Overview of Network Forensics Investigation with a Focus on Peer-to-Peer Networks"**. The First Annual ACM Northeast Digital Forensics Exchange. New York, NY. July 2009.

C. Shields and B.N. Levine,**"Internet Privacy and Anonymity"**. ACM Conference on Computer Communications Security (CCS). October 2004.

C. Shields and B.N. Levine **"Internet Privacy and Anonymity"**. ACM International Conference on Measurements and Modeling of Computer Systems (SIGMETRICS). June 2002.

Exhibit 20

Grants and Funding

Improving Partial Text Matching with Space-efficient Probabilistic Token Storage, Naval Postgraduate School, $331,985

CC-NIE Network Infrastructure: Enabling Big-Data Science Collaboration at Georgetown, National Science Foundation, $379,018

II-NEW: Infrastructure for Change: From a Teaching Department to National Prominence, National Science Foundation, $460,000

Improving Forensic Triage with Rapid Text Document Similarity Matching, Naval Postgraduate School, $383,444, 2010-2013.

Selectable Anonymity for Enabling SAFER Telecommunications (SAFEST), Defense Advanced Research Projects Agency, $1,191,113, 2010-2014.

A System for Identifying and Gathering Evidence of P2P Trafficking, U.S. Department of Justice, Washington, D.C. $227,502 in FY10 and $221,104 allocated for FY11.

Information Assurance Scholarship Program Annex I and Annex II, National Security Agency, Fort Meade, MD, 2009, $19,716 awarded, $405,273 in optional funding pending.

Peerless: A System for Identifying and Gathering Evidence of P2P Tracking, U.S. Department of Justice, Washington, D.C., 2009, $237,834 .

Research Opportunities for Undergraduates, National Science Foundation, Arlington, VA., 2005, $5,625.

Georgetown University Research Opportunities Program Summer Research Fellowship, Spring 2005, $4,000.

Matching Network Data Flows. Georgetown University Research Opportunities Program, Washington, D.C., Spring 2004, $400.

Junior Faculty Research Fellowship, Georgetown University, Washington, D.C. Fall 2003.

Detecting the Sybil Attack in Ad hoc Wireless Networks, Georgetown University Research Opportunities Program, Fall 2003, $400.

Collaborative Research:Anonymous Protocols, National Science Foundation, Arlington, VA. $140,000, 2001.

Courses Taught

Graduate Courses

- Topics in Computer Security: Spring 2013
- Network Security: Spring 2009; Fall 1999 (Purdue)
- Operating Systems: Spring 2000 (Purdue)

Undergraduate Courses

- Information Assurance: Fall 2012, 2010, 2009, 2000 (Purdue); Spring 2006, 2004, 2003, 2002
- Operating Systems: Spring 2012, 2010, 2007, 2005, 2003, 2002
- Computer Networks and Data Communication: Fall 2005, 2004; Spring 2010
- Computer Science 1: Fall 2012, 2010, 2006, 2005, 2004, 2002, 2001
- Operating Systems: 2001 (Purdue)
- Unix for Non-believers: Fall 2009 (with Mark Maloof)

Service

Professional Service

Editor Special Issue of Computer Communications, Volume 29, Number 3, 1 February 2006

Program Chair DFRWS 2012, 2013

Program Committees NDSS 2001,2002; NGC 2001, 2002, 2003; IPCCC 2002;
Security and Assurance in Ad hoc Networks Workshop 2003; CNFR 2005;
SADFE 2009,2010,2011; NeFX 2009, 2010 (Workshop Chair); DFRWS 2009,2010,2011, 2014;
HICSS Forensics Minitrack Co-Chair 2011

Exhibit 20

Reviewer ACM TON, ACM TOM, SPE, IEEE Networks, IEEE Security and Privacy,
Journal of Parallel and Distributed Computing, IEEE TISSEC, IEEE TPDS,
IEEE TDSC, Mobile Information Systems:An International Journal, ACM SIGCOMM,
IEEE INFOCOM, Communciations of the ACM, National Science Foundation

University Service

2002-2003: Freshman advising
2003-2004: Chair of Colloquim Committee, Chair of Curriculum Committee, Merit Review Committee
2004-2005: University Executive Faculty, Chair of Merit Review Committee
2005-2006: University Executive Faculty, Executive Faculty Steering Committee, University Admissions Committee, Chair of Merit Review Committee
2006-2007: Curriculum Committee, University Executive Faculty, Executive Faculty Steering Committee, Search Committee, Web Committee
2007-2008: On sabbatical, University Research Integrity Committee
2008-2009: On parental leave fall semester, Tenure Committee, University Research Integrity Committee
2009-2010: ACM Chapter Advisor, Chair of Search Committee, University Research Integrity Committee, Science in the Public
2010-2011: Chair of Search Committee, Science in the Public Interest Advisory Committee
2011-2012: Chair of Search Committee, Science in the Public Interest Advisory Committee
2012-2013: Chair of Search Committee
2013-2014: Director of Graduate Studies, Faculty IT Advisory Committee

Public Service

Puppy Raiser for Guiding Eyes for the Blind 2001-2003, 2005-2007
Media Appearances CNN 2002, Weird US 2005

Certification

EnCase Certified Examiner (EnCE), 2005
Completed 64 hours of computer forensic training and the EnCase Certified Examiner program.

Exhibit 20

APPENDIX B

Exhibit 20

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
14.01.24 Howard, Patrick
14.04.28 Boyle, John
14.02.05 Simmons, Alison
14.02.06 Martin, Jeff
14.02.14 Bradley, Brandon
14.03.04 Daugherty, Michael LabMD Rule 3.33
14.02.10 Daugherty, Michael
14.02.11 Parr, Jennifer
13.12.02 Dooley, Jeremy
13.11.21 Boback, Robert Tiversa Rule 3.33
13.12.13 Hyer, Robert

Correspondence	**Bates Range**
10.07.16 Ellis Letter	FTC-LABMD-002495-FTC-LABMD-002503

Documents Produced by LabMD

FTC-LABMD-002748-FTC-LABMD-002818
FTC-LABMD-003752-FTC-LABMD-003761

Documents Produced by Cypress Communication, LLC

FTC-CYP-0001735-FTC-CYP-0001757
FTC-CYP-0001790-FTC-CYP-0001791

Exhibit 20

FTC-CYP-0001792-FTC-CYP-0001793

Web Content Considered or Relied Upon

- Archive.org – LimeWire 4.16.6 source code from WayBack machine, http://web.archive.org/web/20081203173114/http://www.limewire.org/limewire.zip, last accessed April 11, 2014.
- Archive.org – LimeWire JavaDoc documentation from WayBack machine, http://web.archive.org/web/20081003012212/http://wiki.limewire.org/index.php?title=Javadocs, last accessed April 11, 2014.
- Archive.org – LimeWire Wiki documentation from WayBack machine, http://web.archive.org/web/20081024044053/http://wiki.limewire.org/index.php?title=Overview, last accessed April 11, 2014.
- Gnutella protocol version 0.4 -- http://rfc-gnutella.sourceforge.net/developer/stable/, last accessed April 11, 2014.
- Gnutella protocol version 0.6 -- http://rfc-gnutella.sourceforge.net/src/rfc-0_6-draft.html, last accessed April 11, 2014.
- Gtk-gnutella protocol, version 1.01 -- http://gtk-gnutella.sourceforge.net/, last accessed April 11, 2014.
- United States Computer Readiness Team – About Us, http://www.us-cert.gov/about-us, last accessed April 11, 2014.
- United States Computer Readiness Team – Security Tip (ST05-007) "Risks of File-Sharing Technology", https://www.us-cert.gov/ncas/tips/ST05-007, last accessed April 11, 2014.

  University of Oregon Department of Computer Science -- Capturing Accurate Snapshots of the Gnutella Network PowerPoint, http://mirage.cs.uoregon.edu/slide/stutzbach_gi_2005.pdf, last accessed April 11, 2014.

Articles & Publications

- Cole, Eric, Ph.D., Security Haven "Security Best Practices" (2006), http://www.securityhaven.com/docs/Security_Best_Practices.pdf, last accessed April 10, 2014.
- Cisco, "Cisco Configuration Professional: Zone-Based Firewall Blocking Peer to Peer Traffic Configuration Example" (December 03, 2010), http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/112237-block-p2p-zbf-ccp-00.pdf, last accessed April 11, 2014.
- Cisco, "Security Device Manager: Block P2P Traffic on a Cisco IOS Router using NBAR Configuration Example" (June 4, 2009), http://www.cisco.com/c/en/us/support/docs/routers/3800-series-integrated-services-routers/110388-ios-block-p2p.html, last accessed April 11, 2014.
- Federal Trade Commission "FTC Issues Report on Peer-to-Peer File Sharing" (June 23, 2005), http://www.ftc.gov/news-events/press-releases/2005/06/ftc-issues-report-peer-peer-file-sharing, last accessed April 11, 2014.

Exhibit 20

- Global Information Assurance Certification Paper "Security Implications of 'Peer-To-Peer' Software" (July 2002), http://www.giac.org/paper/gsec/2016/security-implications-peer-to-peer-software/103490, last accessed April 10, 2014.
- Global Information Assurance Certification Paper "Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications" (December 20, 2003), http://www.giac.org/paper/gsec/3519/security-ramifications-peer-peer-p2p-file-sharing-applications/105733, last accessed April 10, 2014.
- Global Information Assurance Certification Paper "Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment" (2003), http://www.giac.org/paper/gsec/3123/peer-to-peer-p2p-file-sharing-applications-threat-corporate-environment/103882, last accessed April 10, 2014.
- "Information Systems Security, a Comprehensive Model", http://cryptosmith.com/sites/default/files/docs/MccumberAx.pdf, last accessed April 11, 2014.
- Internal Revenue Service "Request for Taxpayer Identification Number and Certification" (November 2005, http://dese.mo.gov/se/documents/se-fs-w9.pdf, last accessed April 11, 2014.
- Ritter, Jordan "Why Gnutella Can't Scale. No, Really." (February 2001), http://www.darkridge.com/~jpr5/doc/gnutella.html, April 11, 2014.
- SANS Institute InfoSec Reading Room "Peer-to-Peer File-Sharing Networks: Security Risks" (2002), https://www.sans.org/reading-room/whitepapers/policyissues/peer-to-peer-file-sharing-networks-security-risks-510, last accessed April 11, 2014.
- SANS Institute InfoSec Reading Room "The Real Cost of Free Programs such as Instant Messaging and Peer-to-Peer File Sharing Applications" (July 1, 2003), https://www.sans.org/reading-room/whitepapers/protocols/real-cost-free-programs-instant-messaging-peer-to-peer-file-sharing-applications-1155, last accessed April 11, 2014.
- Scarfone, Karen, Grance, Tim, Masone, Kelly, National Institute of Standards and Technology "Computer Security Incident Handling Guide" (March 2008), https://www.fismacenter.com/SP800-61rev1.pdf, last accessed April 11, 2014.
- Shanyu Zhao, Daniel Stutzbach, Reza Rejaie, University of Oregon "Characterizing Files in the Modern Gnutella Network: A Measurement Study", http://ix.cs.uoregon.edu/~reza/PUB/tr05-04.pdf, last accessed April 11, 2014.
- Stutzbach, Daniel, and Reza Rejaie, University of Oregon "Capturing accurate snapshots of the Gnutella network" (2005), http://www.barsoom.org/papers/gi05.pdf, last accessed April 11, 2014.

FTC Provided Documents

- 14.04.01 Expert Report of Adam Fisk in the Matter of LabMD, Inc.
- 14.03.03 Respondent's Objections and Responses to Complaint Counsel's Requests for Admission

Exhibit 20

<u>Miscellaneous</u>

- *Arista Records, LLC v. Lime Group LLC*, 715 F. Supp. 2d 481, 96 U.S.P.Q 2d 1437 (S.D.N.Y 2010)

Exhibit 20

EXHIBIT 21

From: Moore, David
Sent: Tuesday, July 29, 2003 1:08:46 PM
To: Distribution
Subject: New CA:File-Sharing: A Fair Share? Maybe Not.

Attachments: ALT128-fileshare.txt; ALT128-fileshare.pdf

Title: File-Sharing: A Fair Share? Maybe Not.
Description: Two page consumer alert warning consumers of the privacy risks of peer-to-peer file sharing
Partners: None
Staff contacts: Carol Kando-Pineda & Carolyn Riley (OCBE); Beth Delaney (DAP)
Status: New
Category: Alert
Stock code: ALT-128
Web File: http://www.ftc.gov/bcp/conline/pubs/credit/bbcr.htm www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm and pdf
Web Menus: Internet; Media Resources; Privacy
Best Sellers: Yes
CIS: Yes
Release date: Immediate
Publication date: July 2003
Print run: 5,000 in house
Distribution: 100 to each RO; 2,000 to B-20; 2,200 to Aspen Systems
Files: TXT and PDF attached

072903

Exhibit 21

FTC Consumer Alert

File-Sharing: A Fair Share? Maybe Not.

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- Set up the file-sharing software very carefully. If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- Be aware of spyware. Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.

- Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- Use and update your anti-virus software regularly. Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Although your virus filter should prevent your computer from receiving possibly destructive files, computer security experts suggest you avoid files with extensions like .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd.

Exhibit 21

- Talk with your family about file-sharing. Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

July 2003

Exhibit 21

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

File-Sharing: A Fair Share? Maybe Not.

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- **Set up the file-sharing software very carefully.** If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- **Be aware of spyware.** Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.

- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- **Use and update your anti-virus software regularly.** Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Although your virus

Exhibit 21

filter should prevent your computer from receiving possibly destructive files, computer security experts suggest you avoid files with extensions like *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*.

- **Talk with your family about file-sharing.** Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION
1-877-FTC-HELP www.ftc.gov

July 2003

Exhibit 21

EXHIBIT 22

From: Moore, David L.
Sent: Thursday, June 23, 2005 1:08:45 PM
To: Distribution
Subject: Revised CA: P2P File-Sharing: Evaluating the Risks

Attachments: ALT128-p2p.txt; ALT128-p2p.pdf

Title: P2P File-Sharing: Evaluating the Risks

Description: Two page consumer alert warning consumers of the privacy risks of peer-to-peer file sharing

Keywords: P2P, file-sharing, privacy

Status: Revised (note: title and boilerplate change only)

Staff contacts: Kial Young (NWR); Nat Wood/Callie Ward (OCBE)

Partners: None

Category: Consumer Alert

Stock code: ALT-128

Web File: www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm and pdf

Web Menus: Internet; Media Resources; Privacy

Best Sellers: No

CIS: No

Release date: immediate

Publication date: June 2005

Sunset date: June 2008

Print run: none (online only)

Distribution: online only

Files: TXT and PDF attached

Exhibit 22

Federal Trade Commission
Consumer Alert

P2P File-Sharing: Evaluating the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- Set up the file-sharing software very carefully. If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- Be aware of spyware. Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.

- Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- Use and update your anti-virus software regularly. Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Although your virus filter should prevent your computer from receiving possibly destructive files, computer security experts suggest you avoid files with extensions like .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd.

Exhibit 22

- Talk with your family about file-sharing. Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

June 2005

Exhibit 22

FTC Consumer Alert

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Office of Consumer & Business Education

P2P File-Sharing: Evaluating the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- Set up the file-sharing software very carefully. If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- Be aware of spyware. Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.

- Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

Exhibit 22

- Use and update your anti-virus software regularly. Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Although your virus filter should prevent your computer from receiving possibly destructive files, computer security experts suggest you avoid files with extensions like .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd.

- Talk with your family about file-sharing. Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission ftc.gov
1-877-FTC-HELP For The Consumer

June 2005

Exhibit 22

EXHIBIT 23

From: Moore, David L.
Sent: Monday, July 18, 2005 7:38:37 PM
To: Distribution
Subject: Revised CA: P2P File-Sharing: Evaluate the Risks

Attachments: ALT128-p2p.txt; ALT128-p2p.pdf; ALT128-p2p.indd

Title: P2P File-Sharing: Evaluate the Risks

Description: Two page consumer alert warning consumers of the privacy risks of peer-to-peer file sharing

Keywords: P2P, file-sharing, privacy, peer-to-peer

Status: Revised

Staff contacts: Kial Young (NWR); Nat Wood/Erin Malick (OCBE)

Partners: None

Category: Consumer Alert

Stock code: ALT-128

Web File: www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm and pdf

Web Menus: already on menus required, so all will update automatically

Best Sellers: No

CIS: No

Release date: immediate

Publication date: July 2005

Sunset date: July 2008

Print run: none (online only)

Distribution: online only

Files: InDesign, TXT and PDF attached (properties updated)

Exhibit 23

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- Set up the file-sharing software very carefully. If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- Be aware of spyware. Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.

- Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- Use an effective anti-virus program and update it regularly. Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Not all anti-virus programs block files downloaded through file-sharing, so check your program's capabilities and settings. In addition, avoid downloading files with extensions

Exhibit 23

like .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd.

- Talk with your family about file-sharing. Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free,
1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

July 2005

Exhibit 23

FTC Consumer Alert

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Office of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- **Set up the file-sharing software very carefully.** If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- **Be aware of spyware.** Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, you may want to buy software that can prevent the downloading of spyware or help detect it on your hard drive.

- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

Exhibit 23

- **Use an effective anti-virus program and update it regularly.** Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Not all anti-virus programs block files downloaded through file-sharing, so check your program's capabilities and settings. In addition, avoid downloading files with extensions like *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*.

- **Talk with your family about file-sharing.** Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

July 2005

Exhibit 23

ALT128-p2p.indd

UNSUPPORTED OR EXCLUDED FILE TYPE

Exhibit 23

Exhibit 24

From:	Holz, Dawne E. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=DHOLZ>
Sent:	Saturday, December 9, 2006 12:07 AM
To:	Distribution <Distribution@ftc.gov>
Subject:	Revised: ALT-128 P2P File-Sharing: Evaluate the Risks
Attach:	alt128-p2p.txt; ALT128-p2p.pdf

Title: P2P File-Sharing: Evaluate the Risks

Description: Warns consumers of the privacy risks of peer-to-peer file sharing; 8.5"x11", 2 pages

Keywords: P2P, file-sharing, privacy, peer-to-peer

Status: Revised. Distribute old copies.

Staff contacts: Erin Malick (DCBE)

Partners: None

1st Category: Computers and the Internet: Entertainment

2nd Category: Computers and the Internet: Privacy and Security

Stock code: ALT-128

Pueblo Ref Number: n/a - not in print

Web File: www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.htm and pdf

Web Menus: Current menus (already updated)

Online Order: No

CIS: No

Release date: Immediate

Publication date: December 2006

Sunset date: December 2007

Print run: none

Packaging: n/a

Min/Max: n/a

Distribution: web only

Files: TXT and PDF attached - **PDF document properties updated**

Exhibit 24

Consumer Alert

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- Set up the file-sharing software very carefully. If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- Be aware of spyware. Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, get an anti-spyware program from a vendor you know and trust. Set it to scan on a regular basis — at least once a week — and every time you start your computer, if possible. And, delete any software programs the anti-spyware program detects that you don't want on your computer.

- Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- Use an effective anti-virus program and update it regularly. Files you download could

Exhibit 24

be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Not all anti-virus programs block files downloaded through file-sharing, so check your program's capabilities and settings. In addition, avoid downloading files with extensions like .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, and .cmd.

- Talk with your family about file-sharing. Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free,
1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission
ftc.gov
1-877-FTC-HELP
For the Consumer

December 2006

Exhibit 24

FTC Consumer Alert

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Division of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. You simply download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free and easily accessible.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share. You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- **Set up the file-sharing software very carefully.** If you don't check the proper settings when you install the software, you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents.

- **Be aware of spyware.** Some file-sharing programs install other software known as spyware. Spyware monitors a user's browsing habits and then sends that data to third parties. Sometimes the user gets ads based on the information that the spyware has collected and disseminated. Spyware can be difficult to detect and remove. Before you use any file-sharing program, get an anti-spyware program from a vendor you know and trust. Set it to scan on a regular basis — at least once a week — and every time you start your computer, if possible. And, delete any software programs the anti-spyware program detects that you don't want on your computer.

- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

Exhibit 24

- **Use an effective anti-virus program and update it regularly.** Files you download could be mislabeled, hiding a virus or other unwanted content. Use anti-virus software to protect your computer from viruses you might pick up from other users through the file-sharing program. Not all anti-virus programs block files downloaded through file-sharing, so check your program's capabilities and settings. In addition, avoid downloading files with extensions like *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*.

- **Talk with your family about file-sharing.** Parents may not be aware that their children have downloaded file-sharing software on the family computer and that they may have exchanged games, videos, music, pornography, or other material that may be inappropriate for them. Also, because other peoples' files sometimes are mislabeled, kids unintentionally may download these files. In addition, kids may not understand the security and other risks involved with file-sharing and may install the software incorrectly, giving anyone on the Internet access to the family's private computer files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

December 2006

Exhibit 24

Exhibit 25

From: Holz, Dawne E. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=DHOLZ>

Sent: Wednesday, April 30, 2008 6:52 PM

To: Distribution <Distribution@ftc.gov>

Subject: Revised: ALT-128 P2P File-Sharing: Evaluate the Risks

Attach: ALT128-p2p.pdf; ALT128-p2p.txt

Title: P2P File-Sharing: Evaluate the Risks

Description: Urges computer users to consider the trade-offs and risks of using peer-to-peer file-sharing. Includes tips to secure your personal information. 8.5" x 11", 2 pages.

Keywords: peer-to-peer, P2P, file, sharing, online, safety, ID theft

Today's Tip: File sharing can give you access to a wealth of information, music, games, and software--but are you sure you're not sharing personal information at the same time? Here are tips to help you make sure you don't get (or give) more than you bargained for. Learn more...

Status: Revised

Staff contacts: Jennifer Leach (DCBE), Carl Settlemeyer (DAP), Stacey Ferguson (DAP)

Partners: None

1st Category: Computers and the Internet: Entertainment

2nd Category: Computers and the Internet: Privacy and Security

Stock code: ALT-128

Pueblo Ref Number: n/a

Web File: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm and pdf

Web Menus: Existing and per categories above

*Note: This information is on OnGuardOnline as the P2P File-Sharing module: http://onguardonline.gov/p2p.html

Online Order: No

CIS: No

Release date: February 2008

Publication date: February 2008

Sunset date: February 2011

Print run: n/a

Packaging: n/a

Exhibit 25

Min/Max: n/a

Distribution: n/a

Files: .pdf and .txt files attached

Exhibit 25

FTC Consumer Alert

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Division of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. To share files through a P2P network, you download special software that connects your computer to other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files – even giving access to entire folders and subfolders – you never intended to share. You may download material that is protected by copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

- **Install file-sharing software carefully, so that you know what's being shared.** When you load a file-sharing application onto your computer, any changes you make to the P2P software's default settings during installation could cause serious problems. For example, if you change the defaults when you set up the "shared" or "save" folder, you may let other P2P users into any of your folders – and all its subfolders. You could inadvertently share information on your hard drive – like your tax returns, email messages, medical records, photos, or other personal documents – along with the files you want to share. And almost all P2P file-sharing applications will, by default, share the downloads in your "save" or "download" folder – unless you set it not to.

- **Use security software and keep it and your operating system up-to-date.** Some file-sharing programs may install malware that monitors a user's computer use and then sends that data to third parties. Files you download may also hide malware, viruses, or other unwanted content. And when you install a P2P file-sharing application, you might be required to install "adware" that monitors your browsing habits and serves you advertising.

  Malware and adware can be difficult to detect and remove. Before you use any file-sharing program, get a security program that includes anti-virus and anti-spyware protection from a vendor you know and trust and make sure that your operating system is up to date. Set your security software and operating system to be updated regularly. Make sure your security software and firewall are running whenever your computer is connected to the Internet. Delete any software the security program detects that you don't want on your computer. And before

Exhibit 25

you open or play any downloaded files, scan them with your security software to detect malware or viruses.

- **Close your connection.** In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or "broadband" connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These "always on" connections may allow others to copy your shared files at any time. To be sure your file-sharing program is closed, take the time to "exit" the program, rather than just clicking "X" or "closing" it. What's more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program's controls to prevent the file-sharing program from automatically opening.

- **Create separate user accounts.** If more than one person uses your computer, consider setting up separate user accounts, in addition to the administrator's account, and give those user accounts only limited rights. Since only a user with administrator rights can install software, this can help protect against software you don't want on your computer. It also can keep users from accessing other users' folders and subfolders, since users with limited rights generally don't have access to each other's information. Also use a password to protect your firewall and security software so no one else can disable them or grant themselves rights that you don't want them to have on your machine.

- **Back up sensitive documents.** Back up files that you'd want to keep if your computer crashes. Store them on CDs, DVDs, or detachable drives that you keep in a safe place.

- **Talk with your family about file-sharing.** If you're a parent, ask your children whether they've downloaded file-sharing software, and if they've exchanged games, videos, music, or other material. Talk to your kids about the security and other risks involved with file-sharing and how to install the software correctly, if they're going to use P2P file-sharing at all. If you're a teen or tween interested in file-sharing, talk with your parents before downloading software or exchanging files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

February 2008

CX0788 page 4

Exhibit 25

FTC Consumer Alert

Federal Trade Commission Bureau of Consumer Protection Division of Consumer & Business Education

P2P File-Sharing: Evaluate the Risks

Every day, millions of computer users share files online. Whether it is music, games, or software, file-sharing can give people access to a wealth of information. To share files through a P2P network, you download special software that connects your computer to other computers running the same software. Millions of users could be connected to each other through this software at one time. The software often is free.

Sounds promising, right? Maybe, but make sure that you consider the trade-offs. The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that file-sharing can have a number of risks. For example, when you are connected to file-sharing programs, you may unknowingly allow others to copy private files – even giving access to entire folders and subfolders – you never intended to share. You may download material that is protected by copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else.

To secure the personal information stored on your computer, the FTC suggests that you:

• Install file-sharing software carefully, so that you know what's being shared. When you load a file-sharing application onto your computer, any changes you make to the P2P software's default settings during installation could cause serious problems. For example, if you change the defaults when you set up the "shared" or "save" folder, you may let other P2P users into any of your folders – and all its subfolders. You could inadvertently share information on your hard drive – like your tax returns, email messages, medical records, photos, or other personal documents – along with the files you want to share. And almost all P2P file-sharing applications will, by default, share the downloads in your "save" or "download" folder – unless you set it not to.

• Use security software and keep it and your operating system up-to-date. Some file-sharing programs may install malware that monitors a user's computer use and then sends that data to third parties. Files you download may also hide malware, viruses, or other unwanted content. And when you install a P2P file-sharing application, you might be required to install "adware"

Exhibit 25

that monitors your browsing habits and serves you advertising.

Malware and adware can be difficult to detect and remove. Before you use any file-sharing program, get a security program that includes anti-virus and anti-spyware protection from a vendor you know and trust and make sure that your operating system is up to date. Set your security software and operating system to be updated regularly. Make sure your security software and firewall are running whenever your computer is connected to the Internet. Delete any software the security program detects that you don't want on your computer. And before

Exhibit 25

you open or play any downloaded files, scan them with your security software to detect malware or viruses.

• Close your connection. In some instances, closing the file-sharing program window does not actually close your connection to the network. That allows file-sharing to continue and could increase your security risk. If you have a high-speed or “broadband” connection to the Internet, you stay connected to the Internet unless you turn off the computer or disconnect your Internet service. These “always on” connections may allow others to copy your shared files at any time. To be sure your file-sharing program is closed, take the time to “exit” the program, rather than just clicking “X” or “closing” it. What’s more, some file-sharing programs automatically open every time you turn on your computer. As a preventive measure, you may want to adjust the file-sharing program’s controls to prevent the file-sharing program from automatically opening.

• Create separate user accounts. If more than one person uses your computer, consider setting up separate user accounts, in addition to the administrator’s account, and give those user accounts only limited rights. Since only a user with administrator rights can install software, this can help protect against software you don’t want on your computer. It also can keep users from accessing other users’ folders and subfolders, since users with limited rights generally don’t have access to each other’s information. Also use a password to protect your firewall and security software so no one else can disable them or grant themselves rights that you don’t want them to have on your machine.

• Back up sensitive documents. Back up files that you’d want to keep if your computer crashes. Store them on CDs, DVDs, or detachable drives that you keep in a safe place.

• Talk with your family about file-sharing. If you're a parent, ask your children whether they've downloaded file-sharing software, and if they've exchanged games, videos, music, or other material. Talk to your kids about the security and other risks involved with file-sharing and how to install the software correctly, if they’re going to use P2P file-sharing at all. If you're a teen or tween interested in file-sharing, talk with your parents before downloading software or exchanging files.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint, or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing,

Exhibit 25

identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database
available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FOR THE CONSUMER1-877-FTC-HELPftc.govFEDERAL TRADE COMMISSION
February 2008

EXHIBIT 26

From: Moore, David L.
Sent: Thursday, August 18, 2005 4:19:01 PM
To: Distribution
Subject: Revised SCA: Uso Compartido de Archivos: Cómo Evaluar los Riesgos (File-Sharing: Evaluate the Risks)

Attachments: salt128-P2P.pdf; salt128-P2P.indd; SALT128 File Sharing Evaluate the Risks.txt

Title: Uso Compartido de Archivos: Cómo Evaluar los Riesgos (File-Sharing: Evaluate the Risks)

Description: Spanish-language version of two page consumer alert warning consumers of the privacy risks of peer-to-peer file sharing

Keywords: P2P, uso compartido de archivos, file-sharing, privacidad, peer-to-peer

Status: Revised.

Staff contacts: Carole Reynolds (FP); Colleen Tressler, Alvaro Puig, David Moore (OCBE)

Partners: None

Category: Consumer Alert

Stock code: SALT-128

Web File: http://www.ftc.gov/bcp/conline/spanish/alerts/s-sharealrt.htm

Web Menus:
http://www.ftc.gov/bcp/conline/edcams/infosecurity/espanol.html
http://www.ftc.gov/bcp/conline/edcams/spam/espanol.htm
http://www.ftc.gov/bcp/conline/edcams/ojo/s-coninfo.htm
http://www.ftc.gov/bcp/menu-internet_span.htm

Best Sellers: No

CIS: No

Release date: Immediate

Publication date: July 2005

Sunset date: July 2008

Print run: None

Packaging: n/a

Distribution: online only

Files: TXT and PDF attached - **PDF document properties updated**

Exhibit 26

Alerta de la FTC para Consumidores

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer & Business Education

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 envía 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.

Exhibit 26

- **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

FEDERAL TRADE COMMISSION ftc.gov
1-877-FTC-HELP FOR THE CONSUMER

Julio 2005

Exhibit 26

salt128-P2P.indd

UNSUPPORTED OR EXCLUDED FILE TYPE

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 envía 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 27

From: Holz, Dawne E. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=DHOLZ>

Sent: Tuesday, February 27, 2007 4:37 PM

To: Distribution <Distribution@ftc.gov>

Subject: Revised: Compartido de Archivos: Cómo Evaluar los Riesgos (File-Sharing: Evaluate the Risks)

Attach: SALT128-P2P.pdf; SALT128-P2P.txt

Title: Uso Compartido de Archivos: Cómo Evaluar los Riesgos (File-Sharing: Evaluate the Risks)

Description: Warns consumers of the privacy risks of peer-to-peer file sharing. 8.5"x11", 2 pages.

Spanish Description: Consejos sobre como usar las redes de archivos compartidos (file sharing networks) de manera segura y proteger su información personal. 8.5"x11", 2 páginas.

Keywords: P2P, uso compartido de archivos, file-sharing, privacidad, peer-to-peer

Status: Revised. Distribute any remaining copies

Staff contacts: Alvaro Puig, Erin Malick (DCBE)

Partners: None

1st Category: Computers and the Internet: Entertainment

2nd Category: Computers and the Internet: Privacy and Security

Stock code: SALT-128

Pueblo Ref Number: n/a (not in print)

Web File: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/salt128.htm and .pdf

Web Menus: (already updated on the following)
http://www.ftc.gov/bcp/conline/edcams/infosecurity/espanol.html
http://www.ftc.gov/bcp/conline/edcams/spam/espanol.htm
http://www.ftc.gov/bcp/conline/edcams/ojo/coninfo.htm
http://www.ftc.gov/bcp/conline/edcams/ojo/s-coninfo.htm
http://www.ftc.gov/bcp/menu-internet_span.htm

Online Order: No

CIS: No

Release date: Immediate

Publication date: October 2006

Sunset date: October 2007

Print run: None

Exhibit 27

Packaging: n/a

Min/Max: n/a

Distribution: n/a

Files: TXT and PDF attached - **PDF document properties updated**

Exhibit 27

Alerta de la FTC para Consumidores

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

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 espionaje (*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 envía 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, compre un programa *anti-spyware* en un negocio conocido que le inspire confianza. Instálelo para que examine su computadora regularmente — por lo menos una vez por semana — y si fuera posible, cada vez

Exhibit 27

que encienda su computadora; por último, elimine todos los programas software que detecte el programa *anti-spyware* que usted no desee conservar en 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.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

Octubre 2006

Exhibit 27

Alerta de la FTC para Consumidores

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer & Business Education

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 espionaje (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 envía 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, compre un programa anti-spyware en un negocio conocido que le inspire confianza. Instálelo para que examine su computadora regularmente — por lo menos una vez por semana — y si fuera posible, cada vez que encienda su computadora; por último, elimine todos los programas software que detecte el programa anti-spyware que usted no desee conservar en 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.

Octubre 2006

Exhibit 27

EXHIBIT 28

From:	Holz, Dawne E. </O=FTCEXCHANGE/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=DHOLZ>
Sent:	Wednesday, April 30, 2008 6:53 PM
To:	Distribution <Distribution@ftc.gov>
Subject:	Revised: SALT-128 Uso Compartido de Archivos: Cómo Evaluar los Riesgos (P2P File-Sharing: Evaluate the Risks)
Attach:	SALT128-P2P.pdf; SALT128-P2P.txt

Title: Uso Compartido de Archivos: Cómo Evaluar los Riesgos (P2P File-Sharing: Evaluate the Risks)

Description: Urges computer users to consider the trade-offs and risks of using peer-to-peer file-sharing. Includes tips to secure your personal information. 8.5" x 11", 2 pages.

Description in Spanish: Alienta a los consumidores a considerar las ventajas y los riesgos del uso compartido de archivos, o P2P. Incluye consejos sobre cómo proteger su información personal. 8.5" x 11", 3 páginas.

Keywords: uso, compartido, archivos, P2P, seguridad, Internet, robo, identidad

Today's Tip: El uso compartido de archivos puede darle acceso a una gran cantidad de información - música, juegos, y programas de computadora - ¿pero esta seguro que no esta compartiendo su información personal al mismo tiempo? Sigua estos consejos para asegurarse de que no este compartiendo - o recibiendo - más de lo que se imaginaba. Aprenda más.

Status: Revised

Staff contacts: Jennifer Leach/Alvaro Puig (DCBE), Carl Settlemeyer/Stacey Ferguson (DAP)

Partners: None

1st Category: Computadoras y el Internet: Entretenimiento

2nd Category: Computadoras y el Internet: Privacidad y Seguridad

Stock code: SALT-128

Pueblo Ref Number: n/a

Web File: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/salt128.shtm and pdf

Web Menus: Existing and per categories above

*Note: This information is on OnGuardOnline as the P2P File-Sharing module: http://alertaenlinea.gov/uso_compartido.html.

Online Order: No

CIS: No

Release date: February 2008

Publication date: February 2008

Exhibit 28

Sunset date: February 2011

Print run: n/a

Packaging: n/a

Min/Max: n/a

Distribution: n/a

Files: .pdf and .txt files attached

Exhibit 28

Alerta de la FTC para Consumidores

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Division of Consumer & Business Education

Uso Compartido de Archivos: Cómo Evaluar los Riesgos

File-Sharing: Evaluate the Risks

Todos los días, millones de usuarios comparten sus archivos en línea. Ya se trate de música, juegos o programas software, el intercambio de archivos permite que los usuarios de una red P2P intercambien un gran caudal de información. Para poder compartir archivos en una red P2P, usted descarga un programa software especial que conecta su computadora con otras computadoras que operan el mismo software. Por medio de este programa software millones de usuario pueden conectarse entre sí al mismo tiempo. Frecuentemente, este programa es gratis.

¿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 una red P2P, sin darse cuenta puede permitir que otros usuarios copien sus archivos privados – o hasta podría estar abriéndoles la puerta a todas sus carpetas y subcarpetas – que usted no tiene ninguna intención de compartir. Con este software usted podría descargar material protegido por las leyes de derechos de autoría y verse complicado en problemas legales. Usted podría descargar un virus informático o facilitar una violación de seguridad informática; o tal vez podría llegar a descargar involuntariamente pornografía que aparece etiquetada bajo otros títulos.

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

- **Instale el programa de uso compartido de archivos con mucho cuidado para saber qué es lo que esta compartiendo.** Cuando usted descarga a su computadora la aplicación "compartir archivos", cualquiera de los cambios que haga a las características predeterminadas del software P2P durante la instalación podría causarle serios problemas. Por ejemplo, si usted hace cambios a la configuración predeterminada para configurar los tipos de carpetas "guardar" (save) o "compartido" (shared) puede permitir que los demás usuarios de la red P2P accedan a cualquiera de sus carpetas – y a todas sus subcarpetas. De esta manera, junto con los archivos que sí desea compartir, podría estar compartiendo involuntariamente la 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. Casi

CX0789 page 3
Exhibit 28

todas las aplicaciones de los programas de uso compartido de archivos vienen configuradas para compartir los archivos que descargue en su carpeta "guardar" o "descargar", excepto que usted las configure de otra manera.

- **Use un programa de seguridad y manténgalo actualizado y haga lo mismo con su sistema operativo.** Algunos programas de uso compartido de archivos pueden instalar un programa malicioso o malware que monitorea las computadoras de los usuarios y que envía datos a terceros. Los archivos que usted descarga también pueden ocultar malware, virus u otros contenidos indeseables. Además, cuando usted instala un programa P2P para compartir archivos puede que obligatoriamente también instale un "adware", que es un software que monitorea sus hábitos de navegación y le envía publicidad.

  Los programas malware y adware pueden ser difíciles de detectar y eliminar. Antes de usar un programa de uso compartido de archivos, compre un programa de seguridad que incluya protección antivirus y anti-spyware en un negocio conocido que le merezca confianza y controle que su sistema operativo esté actualizado. Configure su software de seguridad y su sistema operativo de manera que se actualice regularmente. Asegúrese de que su software de seguridad y firewall estén activados cuando tenga la computadora conectada al Internet. Elimine todos los programas que detecte el software de seguridad que no desee conservar en su computadora. Y antes de abrir o ejecutar los archivos descargados, escanéelos con el programa de seguridad para detectar si tienen malware o virus.

- **Cierre su conexión.** En algunas instancias, cerrar la ventana del programa de uso compartido de archivos no cierra realmente su conexión con la red. Esto permite que continúe activado el intercambio de archivos, lo cual podría incrementar su riesgo de seguridad. Si usted tiene una conexión de Internet de alta velocidad o banda ancha (high-speed o broadband connection) continuará conectado al Internet a menos que apague su computadora o desconecte su servicio de Internet. Este tipo de conexión que esta siempre activa puede permitir que otros usuarios copien sus archivos en cualquier momento. Para estar seguro de cerrar correctamente su programa P2P, en lugar de hacer clic sobre la "X" o "cerrar", tómese el tiempo de "salir" del programa. 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.

- **Cree cuentas separadas de usuario.** Si usted comparte su computadora con otras personas, además de establecer su propia cuenta de usuario administrador, considere establecer cuentas de usuario por separado para los demás y conceda derechos limitados a esos usuarios. Como la única persona que tiene derecho a instalar programas en la computadora es el usuario administrador, usted evitará que otros lo hagan y así podrá protegerse contra los riesgos que presentan los programas que no desea instalar. De esta manera, también impedirá que los usuarios secundarios accedan a las carpetas y subcarpetas de los otros usuarios, ya que en general, los usuarios con derechos limitados no pueden acceder a la información de los demás. Además, use una contraseña para proteger el firewall y software de seguridad instalado en su computadora para que ninguna otra persona pueda desactivarlos o atribuirse derechos para controlar su computadora que usted no desea concederles.

- **Haga copias de los documentos que contengan información delicada.** Haga copias de seguridad de los archivos que desee preservar en caso de que su computadora sufra un ataque o colapse. Guarde sus documentos importantes en discos CD, DVD o en dispositivos de almacenamiento removibles para guardarlos en un lugar seguro.

- **Hable con su familia sobre el P2P.** Si tiene hijos que usan la computadora, pregúnteles si descargaron un software de uso compartido de archivos y si han estado intercambiando juegos, videos, música o algún otro material. Hable con sus hijos sobre la seguridad y otros riesgos que acarrea compartir archivos y, si de todas maneras van a instarlo y usarlo, dígales cómo deben hacerlo correctamente. Si eres adolescente o un poco más chico y estás interesado en compartir archivos, habla con tus padres antes de descargar el programa P2P o de intercambiar archivos.

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.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

Febrero 2008

Alerta de la FTC para Consumidores

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer & Business Education

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 espionaje (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 envía 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, compre un programa anti-spyware en un negocio conocido que le inspire confianza. Instálelo para que examine su computadora regularmente — por lo menos una vez por semana — y si fuera posible, cada vez que encienda su computadora; por último, elimine todos los programas software que detecte el programa anti-spyware que usted no desee conservar en 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.

Octubre 2006

EXHIBIT 29

CONFIDENTIAL – REDACTED IN ENTIRETY

EXHIBIT 30

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

Exhibit 30

the time of events described in the document?

A Yes.

Q Do you have personal knowledge of the information contained in CX0097?

A Yes.

Q Has CX0097 been maintained by the Sacramento Police Department?

A Yes.

Q I'm handing you a document that's been marked as CX0092.

(Exhibit CX0092 was marked for identification.)

BY MS. VANDRUFF:

Q I'm going to ask you to take a moment, please, to review CX0092.

A Okay.

Q Have you had an opportunity to review CX0092?

A Yes.

Q What is it?

A It's my observations of our initial response and then locating of evidence and seizure of evidence from 5661 Wilkinson Street.

Q Is CX0092 a true and accurate copy of your observations regarding your initial response and your seizure of evidence?

A Yes.

Q Is CX0092 a record that was created by the Sacramento Police Department in the ordinary course of the police department's activities?

A Yes.

Q Is CX0092 a record that was created at or near the time described in the document?

A Yes.

Q Do you have personal knowledge of the information contained in CX0092?

A Yes.

Q Has CX0092 been maintained by the Sacramento Police Department?

A Yes.

Q I believe it was your testimony, Detective Jestes, that at the time of your search of the residence at 5661 Wilkinson Street you identified documents that led you to conclude that identity theft might be occurring; is that correct?

A Yes.

Q What types of materials did you find during your search of the premises at 5661 Wilkinson Street?

A We found checks that appeared to have been washed, and that means that the original ink -- somebody had tried to get rid of the original ink and write new

information on the check.

We also found checks that had preprinted customer information, and there was new printing added to that customer information.

We found bills in other peoples' names for various -- the utility bills and various other things.

We found mail.

We found checks made out to a company called LabMD and then also found several sheets of paper that had what appeared to be social security numbers and names associated with the same LabMD.

Q I'll ask you questions about some of those materials that you found, but before we move on, I'd like you to take a moment to review a document that has been marked as CX0090.

(Exhibit CX0090 was marked for identification.)

BY MS. VANDRUFF:

Q I've handed you CX0090, Detective Jestes, and I'd ask you to take a moment to please review that document.

A Okay.

Q What is CX0090?

A It's a statement that Officer Morgan took from Suspect Erick Garcia.

Q Is CX0090 a true and accurate copy of the

statement that Officer Morgan took from Mr. Garcia?

A Yes.

Q Is CX0090 a record that was created by the Sacramento Police Department in the ordinary course of business?

A Yes.

Q Is CX0090 a record that was created at or near the time of the events described in the document?

A Yes.

Q Has CX0090 been maintained by the Sacramento Police Department?

A Yes.

Q Detective Jestes, I'm handing you a document that's been marked as CX0091, and I'll ask you to take a moment to please review it.

A Okay.

(Exhibit CX0091 was marked for identification.)

BY MS. VANDRUFF:

Q What is CX0091?

A This is a statement that Officer Baptista took from Suspect Josie Maldonado.

Q Is the statement that Officer Baptista took from Ms. Maldonado -- let me ask that differently.

Is CX0091 a true and accurate copy of the

Exhibit 30

41

BY MS. VANDRUFF:

Q Did Detective Shim evaluate the browsing history of the computers during his forensic examination?

MS. HARRIS: Objection to the extent it calls for speculation.

THE WITNESS: Yes.

BY MS. VANDRUFF:

Q What did he find?

A That -- the specific items mentioned were a search about a social security number and a child and then a search of FTC and identity theft.

Q Directing your attention to page 4 of the document that has been marked as CX0100, did Detective Shim also find information regarding the FTC's Web site as it relates to peer-to-peer file-sharing applications?

A Yes.

Q I'm handing you a document that's been marked as CX0101.

(Exhibit CX0101 was marked for identification.)

BY MS. VANDRUFF:

Q I'll ask you to take a moment please to review the document.

A Okay.

42

Q What is CX0101?

A This is also part of the examination of the computer conducted by Detective Shim.

Q Does CX0101 relate to one or both of the computers?

A It's just one of the computers.

Q Which computer does it relate to?

A The desktop.

Q Is CX0101 a true and accurate copy of the report that Detective Shim created related to the desktop computer?

A Yes.

Q Is CX0101 a record that was created by the Sacramento Police Department in the ordinary course of the police department's activities?

A Yes.

Q Is CX0101 a record that was created at or near the time of the events described in the document?

A Yes.

Q Has CX0101 been maintained by the Sacramento Police Department?

A Yes.

Q Let's shift gears and talk about Mr. Garcia and Ms. Maldonado for a moment.

A Okay.

43

Q Prior to October 5th, 2012, had Mr. Garcia been charged with any other crimes?

A Yes.

Q What other crimes?

A Drug offenses and a receiving stolen property offense.

Q Had he been convicted of either of those crimes?

A Yes.

Q Of which crimes was he convicted?

A Both of them. I'm pretty sure both of them.

Q Prior to October 5th, 2012, had Ms. Maldonado been charged with any other crimes?

A Yes.

Q What crimes?

A Possession of narcotic paraphernalia.

Q Had she been convicted?

A If I remember correctly, she -- that one was dismissed.

Q Do you know whether Mr. Garcia and Ms. Maldonado were prosecuted for the crimes for which they were arrested on October 5th, 2012?

A Yes.

Q What was the disposition of Mr. Garcia's case?

A He pled no content and was sentenced to probation and sheriff's work project.

44

Q Did Mr. Garcia's plea of no contest relate to all four of the charges on which he was held on October 5th, 2012?

A No.

Q On which charge did he plead no contest?

A Identity theft.

Q What was the disposition of Ms. Maldonado's case?

A She also pled no contest to identity theft.

Q The identity theft crimes to which Mr. Garcia and Ms. Maldonado pled no contest -- were those felonies?

A Yes.

Q Can identity theft be prosecuted as a misdemeanor?

A I think so.

Q You've described Mr. Garcia and Ms. Maldonado's pleas as no contest.

I understand that under California law it is formally a plea of nolo contendere; is that correct?

A Yes.

Q What is the effect of a plea of nolo contendere?

A They're admitting that they committed the crime, but they're avoiding a trial. This is very layman's terms.

Q Is it different in any material respect from a plea of guilty?

Exhibit 30

EXHIBIT 31

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SACRAMENTO
MINUTE ORDER - PROCEEDINGS

GARCIA ERICK 1 3235091 12F06719 MUNI

Lauren Miller, DDA R. Cohen, PD

DATE	JUDGE	DEPT	REL	CSR	PROCEEDINGS
[illegible] 6 20[illegible] 08:30	MCCORMICK	08	~~Bond~~ EXON	8687	SC (CTS 10): Δ present w/ R. Cohen
					Ms. Diaz of Act Fast Bail Bonds
					surrendered bond. Bond exonerated.
					Δ remanded. Δ noticed bail hrg.
					SC/BR 1-23-13 8:30 8 Δ OTA
1/23/13	WHITE, L.	8	IC	4695	SC/B.R. (Cts-18): Δ present w/cnsl.
					Δ oral request for release on OR put
(Π to have plea offer at next appr.)					over for handling DDA to be present.
					SC/Bail mtn 1-30-13 8:30 8 Δ OTA
[illegible]	White, Laurel	8	~~IC~~ OR	4695	SC/BR (CTS 25): Δ present w/cnsl.
					Π stipulated to OR release.
					Δ released OR.
					SC 2-20-13 8:30 8 Δ OTA
2 0 2013	L. WHITE	8	OR	5034	SC (CTS 25): 3-6-13 8:30 8 plea set AOTA
3/6/13	White L.	8	OR	4695	Plea Set (Cts-25): Δ present w/cnsl.
					Plea entered - see separate minute order.

DEFT ADVISED AND PROVIDED WITH 12021 PC FIREARMS PROHIBITION PACKET

If not already collected, defendant to submit DNA samples purs 296 PC et. seq.

~~□ In Main Jail while in custody~~
☒ Designated out-of-custody facility

no obj to swp/WF

Certified to Superior Court for Immediate J&S;
~~Deft wvd referral to PO and time for J&S;~~
Request Immediate J&S

Δ agreed to pay restitution to victims in SPD report # 12276115.

✓ PO REPORT FILED
✓ J&S 5 YRS ✓ FORMAL ~~___ INFORMAL PROBATION,~~
✓ OAL
180 DAYS CJ ___ C/S ___ C/C; CTS 25 DAYS (+24 GT/WT)
___ SWP REC ___ WF REC, STAY 4-10-13 @RCCC at 6pm
___ APPLY FROM WITHIN ✓ O.R.'D TO APPLY
~~___ DEFT TO PAY FINE OF ___ + PA ___ + CIF ___~~
OR SERVE ___ DAYS CJ C/S; DEFT ELECTS TIME
DEFT ELECTS FINE ___ THRU DRR ___ PAY F/W ___
✓ ALL COND OF PO REPORT PAGES 1 THRU 9 as [redacted]
✓ PAY PROB COSTS THRU DRR; ___ PROB COSTS WVD
✓ DEFT OTR PO [redacted] by 3 pm today.

Exhibit 31

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SACRAMENTO
MINUTE ORDER - PLEA

GARCIA ERICK 1 3235091 12F05719 MUNI

PLEA DATE: 3-6-13 JUDGE: LAUREL D. WHITE DEPT: 8

RIGHTS:

ADV	WVD	
✓		COUNSEL, retained or appointed
✓	✓	PRELIMINARY HEARING
✓	✓	JURY TRIAL, speedy and public
✓	✓	CONFRONTATION, of witness
✓	✓	SELF INCRIMINATION, remain silent

ADVISED

✓ possible maximum sentence
___ possibility of 1203.03 PC
___ parole rights
___ option of changing plea in re: West
✓ consequences of plea

✓ If you are not a citizen, you are hereby advised that conviction of the offense for which you have been charged may have the consequences of deportation, exclusion from admission to the United States, or denial of naturalization pursuant to the laws of the United States.

___ Video mass advisement transcript on request
___ Tape Number ___
✓ Court Reporter (transcript on request) B. Waldron, #4695
___ The written Waiver and Plea form filed herein is ordered incorporated in the record

Defendant advised of above rights, penalties and consequences of plea. Court found defendant understood same. Court found that defendant knowingly, intelligently, voluntarily and expressly waived the rights as indicated by initials above. Defendant entered a plea of:

(5FP 180)

___ GUILTY

✓ NOLO CONTENDERE (acknowledged it is same as guilty)

___ NGRI (PC 1026)

to the charges of: Ct. 1, PC 530.5(a), a felony

BAC: ___

Court dismissed: Cts 2, 3 + 4 w/ Harvey waiver

___ Insufficient Evidence
✓ Interest of Justice
✓ In View of Plea ___
___ Proof Shown
✓ Harvey Waiver Cts 2, 3 + 4 and SPD report #12276115

Court found that the above plea(s) was voluntary and there was a factual basis for same.

Exhibit 31

EXHIBIT 32

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SACRAMENTO
MINUTE ORDER - HEADER/PROCEEDINGS

DEFENDANT NAME	DEF	XREF	CASE
MALDANADO JOSIE MARTINEZ	2	2885371	12F06719 MUNI

CUSTODY STATUS: CUST
DOB: 06/05/1981
LEA: SACRAMENTO POLICE DEPARTMENT
BAIL SET: $35,500.00
BAIL POSTED:

DATE FILED: 10/10/2012
ARREST #: 09715550-01

BOND #:

PROSECUTOR: TEAM 1/TU

DEFENSE: ~~NICHOLSON, , DANIEL~~ Robert Mathew
TYPE: CAC

SECTION(S) VIOLATED:

10/05/2012	(CT 1)	PC	530.5(A)
10/05/2012	(CT 2)	PC	496(A)
10/05/2012	(CT 3)	HS	11377(A)
10/05/2012	(CT 4)	HS	11364.1(A)

DATE	JUDGE	DEPT	REL	CSR	PROCEEDINGS
032013	WHITE , Laurel	08	1/c	4695	SC (CTS 1l)(NO FILE): Robert Mathew
08:30					appearing as Δ's new counsel from the
	~~(co-Δ next appr [illegible])~~ (co-Δ pled)				CCD Panel.
					plea 3-27-13 8:30 8 Δ OTA
3-27-13	Sapunor	8	1/c	4695	PLEA (CTS 1l): Plea entered see separate
					plea sheet Certified to Superior Court for immediate J&S;
					Deft wvd referral to PO and time for J&S;
					~~Request immediate J&S~~ FAW

~~not already collected, defendant to submit~~
A samples purs 296 PC et. seq.
In Main Jail while in custody
~~Designated out-of-custody facility~~

DEFT ADVISED AND PROVIDED WITH 12021 PC FIREARMS PROHIBITION PACKET

* NO obj to SWP/WF/HO

Ct 1

✓ ~~PO REPORT~~ Cond. FILED
✓ J&S 5 YRS ✓ FORMAL ___ INFORMAL PROBATION
✓ OAL
210 DAYS CJ ✓ C/S ___ C/C; CTS 18 DAYS (18+18 = 36 [illegible]
___ SWP REC ___ WF REC, STAY 5-24-13 @RCCC 6pm
___ APPLY FROM WITHIN ✓ O.R.'D TO APPLY
___ DEFT TO PAY FINE OF ___ + PA ___ + CIF ___
OR SERVE ___ DAYS CJ C/S; DEFT ELECTS TIME
DEFT ELECTS FINE ___ THRU DRR ___ PAY F/W ___
✓ ALL COND OF PO REPORT PAGES 1 THRU 6 as mod.
✓ PAY PROB COSTS THRU DRR; ___ PROB COSTS WVD
✓ DEFT OTR PO W/IN ___ ~~DAYS/HOURS OF~~ RELEASE 48 Hrs of release

Cts 2, 3, 4 Dism 1O5/ILOP w/ Harvey waiver P3.

P D not to be release on OR - no obj - gtd

JICR0420/CR61A - PAGE 01

Exhibit 32

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SACRAMENTO
MINUTE ORDER - PLEA

MALDANADO JOSIE MARTINEZ 2 2885371 12F06719 MUNI

PLEA DATE: 3-27-13 JUDGE: JACK V. SAPUNOR DEPT: 8

RIGHTS:

ADM	WVD		ADVISED	
PB		COUNSEL, retained or appointed	PB	possible maximum sentence
	PB	PRELIMINARY HEARING		possibility of 1203.03 PC
		JURY TRIAL, speedy and public		parole rights
		CONFRONTATION, of witness		option of changing plea
		SELF INCRIMINATION, remain silent		in re: West
			PB	consequences of plea

PB If you are not a citizen, you are hereby advised that conviction of the offense for which you have been charged may have the consequences of deportation, exclusion from admission to the United States, or denial of naturalization pursuant to the laws of the United States.

____ Video mass advisement transcript on request
✓ Tape Number ________
____ Court Reporter (transcript on request) B. Waldron #4695
____ The written Waiver and Plea form filed herein is ordered incorporated in the record

Defendant advised of above rights, penalties and consequences of plea. Court found defendant understood same. Court found that defendant knowingly, intelligently, voluntarily and expressly waived the rights as indicated by initials above. Defendant entered a plea of:

Ct 1 - NC
210 Dys No SD
Rest - Victims

____ GUILTY

✓ NOLO CONTENDERE (acknowledged it is same as guilty)

____ NGRI (PC 1026)

to the charges of: Ct PC 530.5 (A) as felony

BAC: ________

Court dismissed: Cts 2, 3, 4 w/ Harvey waiver

____ Insufficient Evidence
✓ Interest of Justice
✓ In View of Plea ________
____ Proof Shown
✓ Harvey Waiver 2, 3, 4

Court found that the above plea(s) was voluntary and there was a factual basis for same.

Exhibit 32

EXHIBIT 33

BUSINESS

Federal Trade Commission For The Consumer

1-877-FTC-HELP www.ftc.gov

FTC FACTS for Business

Security Check: Reducing Risks to your Computer Systems

When consumers open an account, register to receive information or purchase a product from your business, it's very likely that they entrust their personal information to you as part of the process. If their information is compromised, the consequences can be far – reaching: consumers can be at risk of identity theft, or they can become less willing – or even unwilling – to continue to do business with you.

These days, it's just common sense that any business that collects personal information from consumers also would have a security plan to protect the confidentiality and integrity of the information. For financial institutions, it's an imperative: The Gramm-Leach-Bliley Act and the Safeguards Rule, enforced by the Federal Trade Commission, require financial institutions to have a security plan for just that purpose.

The threats to the security of your information are varied – from computer hackers to disgruntled employees to simple carelessness. While protecting computer systems is an important aspect of information security, it is only part of the process. Here are some points to consider – and resources to help – as you design and implement your information security plan.

Starting Out

Sound security for businesses means regular risk assessment, effective coordination and oversight, and prompt response to new developments. Basic steps in information security planning include:

- identifying internal and external risks to the security, confidentiality and integrity of your customers' personal information;
- designing and implementing safeguards to control the risks;
- periodically monitoring and testing the safeguards to be sure they are working effectively;
- adjusting your security plan according to the results of testing, changes in operations or other circumstances that might impact information security; and
- overseeing the information handling practices of service providers and business partners who have access to the personal information. If you give another organization access to your records or computer network, you should make sure they have good security programs too.

Exhibit 33

When setting up a security program, your business should consider all the relevant areas of its operations, including employee management and training; information systems, including network and software design, and information processing, storage, transmission and disposal, and contingencies, including preventing, detecting and responding to a system failure. Although the security planning process is universal, there's no "one size fits all" security plan. Every business faces its own special risks. The administrative, technical, and physical safeguards that are appropriate really depend on the size and complexity of the business, the nature and scope of the business and the sensitivity of the consumer information it keeps.

Determining Priorities Among Risks: Computer Systems

Although computer systems aren't your only responsibility related to information security, they are an important one. With new vulnerabilities announced almost weekly, many businesses may feel overwhelmed trying to keep current. Guidance is available from leading security professionals who put together consensus lists of vulnerabilities and defenses so that every organization, regardless of its resources or expertise in information security, can take basic steps to reduce its risks. The lists identify the commonly exploited vulnerabilities that pose the greatest risk of harm to your information systems. Use these lists to help prioritize your efforts so you can tackle the most serious threats first.

- **The 20 Most Critical Internet Security Vulnerabilities** (www.sans.org/top20) was produced by the SANS Institute and the FBI. It describes the 20 most commonly exploited vulnerabilities in Windows and UNIX. Although thousands of security incidents affect these operating systems each year, the majority of successful attacks target one or more of the vulnerabilities on this list. This site also has links to scanning tools and services to help you monitor your own network vulnerabilities at www.sans.org/top20/tools.pdf.
- **The 10 Most Critical Web Application Security Vulnerabilities** (www.owasp.org) was produced by the Open Web Application Security Project (OWASP). It describes common vulnerabilities for web applications and databases and the most effective ways to address them. Attacks on web applications often pass undetected through firewalls and other network defense systems, putting at risk the sensitive information that these applications access. Application vulnerabilities are often neglected, but they are as important to deal with as network issues.

While you are designing and implementing your own safeguards program, don't forget that you should oversee service providers and business partners that have access to your computer network or consumers' personal information. Check periodically whether they monitor and defend against common vulnerabilities as part of their regular safeguards program.

For more information on privacy, information security, and the Gramm-Leach-Bliley Safeguards Rule, visit www.ftc.gov/privacy.

For More Information

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

June 2003

Exhibit 33

Exhibit 34

PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS, AND THE CENSUS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

on

PROTECTING INFORMATION SECURITY AND PREVENTING IDENTITY THEFT

September 22, 2004

Exhibit 34

I. INTRODUCTION

Mr. Chairman, and members of the subcommittee, I am Commissioner Orson Swindle.[1] I appreciate the opportunity to appear before you today to discuss the Commission's role in promoting information security and combating identity theft.

The Federal Trade Commission has a broad mandate to protect consumers from unfair and deceptive practices. As part of its mission, the Commission has given a special emphasis to efforts to protect the privacy and security of consumer information. These efforts include educating companies about the importance of using reasonable and appropriate procedures to safeguard consumers' personal information, supplemented by law enforcement in appropriate cases when companies fail to take such steps. In addition, as the federal government's central repository for identity theft complaints, the Commission plays a significant role in referring complaints about identity theft to appropriate law enforcement authorities, providing victim assistance and consumer education, and working with businesses to mitigate harm in the event of a security breach.[2]

II. THE BENEFITS AND RISKS OF ELECTRONICALLY-STORED CONSUMER DATA

Electronic information systems provide enormous benefits to consumers, businesses, and government alike. We rely on them for the orderly operation of our financial systems and power supplies, the efficient processing of our transactions, twenty-four hour access to information, and many other conveniences and cost savings. In order to provide these benefits, these computer-driven systems store voluminous data on consumers – ranging from sensitive medical and financial records to catalog purchases. If not adequately protected, these systems and databases can be extremely vulnerable, thus threatening the security of the information they store and

Exhibit 34

maintain.

In particular, a large database containing sensitive personal information can be a treasure trove for identity thieves.[3] When breached, the data in these systems can be used to impersonate consumers, take over their accounts, and cause substantial injury to consumers, businesses, and other institutions.[4] In recent years, there have been reports of a number of large-scale computer security breaches in which identity thieves and others gained access to the sensitive personal information of tens of thousands of consumers. Examples of publicly reported breaches include the theft of computer equipment containing detailed health insurance or financial information, security breaches that exposed credit card data, and the hacking of university databases. Breaches such as these create the potential for – and sometimes result in – mass-scale identity theft with millions of dollars in false charges.

Electronic systems and databases face diverse security threats. Sometimes, companies simply fail to properly safeguard consumers' information, leaving it vulnerable to hackers. Other breaches are caused by insiders, who exploit security weaknesses or use their position and access to the company's systems to steal data. In some instances, the breach can be as simple as the failure to dispose of sensitive documents properly. The adverse consequences of poor security can include not only identity theft and fraud, but also diminished computer operation, spam, "phishing" attacks, or even the takeover of computers to launch attacks on other commercial websites or on parts of the nation's critical information infrastructure.

III. PREVENTING BREACHES AND IDENTITY THEFT

Companies that process or store personal information about consumers – especially sensitive information such as a Social Security number or credit card information – have a

Exhibit 34

responsibility to safeguard that data. The Commission actively attempts to educate businesses and consumers about information security risks and the precautions they must take to protect or minimize risks to personal information. Our emphasis is on preventing breaches before they happen by encouraging businesses and consumers to make security part of their daily routines. We also provide advice to businesses and consumers in the event that a breach involving sensitive personal information does occur.

A. Reasonable Security Procedures

The Commission has considerable experience in understanding and addressing information security concerns. For example, in 1999, the Commission convened an Advisory Committee on Online Access and Security, in which a panel of experts examined the parameters of appropriate security for information collected online and provided a report with its findings.[5] The Commission also drafted and enforces its Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule"), which became effective in 2003.[6] This Rule requires "financial institutions" subject to the FTC's jurisdiction, which includes a broadly-defined group of non-bank entities, to develop and implement appropriate safeguards to protect customer information. In addition, the Commission played a leading role in developing and implementing the Organization for Economic Cooperation and Development's ("OECD") Security Guidelines.[7]

Through this work, as well as our more general education and enforcement initiatives, the Commission has come to recognize several principles that should govern any information security program. First, information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve. Second, a company's security procedures must be reasonable and

Exhibit 34

appropriate in light of the circumstances. Such circumstances include the company's size and complexity, the nature and scope of its activities, and the sensitivity of the consumer information it handles. Third, the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. Finally, a company's practices may be unreasonable even without a known breach of security. Indeed, because the primary purpose of information security is to prevent breaches before they happen, companies cannot simply wait for a breach to occur before they take action.

Implementation of these principles requires businesses to develop a security plan and make security monitoring and oversight part of their regular operations – literally, a part of their culture. Information security planning should include: identifying internal and external risks to the security, confidentiality, and integrity of consumers' personal information; designing and implementing safeguards to control these risks; periodically monitoring and testing the safeguards to be sure they are working effectively; adjusting security plans according to the results of testing or changes in circumstances; and overseeing the information handling practices of service providers who have access to the personal information. As discussed below, these basic steps are required by the Commission's Safeguards Rule and the Commission's orders in cases involving information security.

B. Managing a Data Compromise

Companies should implement reasonable security procedures to prevent the compromise of sensitive personal information. In the event that a security breach does occur, however, there are several steps businesses should take to respond.[8]

Exhibit 34

For example, if the security breach could result in harm to a person or business, companies should report the situation to the appropriate law enforcement agency. Companies should also consider whether the data compromise may affect other businesses, and if so, should notify them. In particular, if a breach affects information that a company stores or maintains on behalf of another business, notification to the other business would be appropriate.

In addition, companies should evaluate whether to notify consumers that there has been a breach.[9] For example, consumer notification may not be necessary if the information is not sensitive or there is no evidence of unauthorized access. If information that creates a risk of identity theft has been stolen, however, the FTC suggests notifying individuals of the incident as soon as possible so they can take steps to limit the potential damage.[10] For example, if an individual's Social Security number is compromised, that individual, by placing a fraud alert on his credit file, will have a good chance of preventing, or at least reducing, the likelihood of identity theft or the misuse of this information.[11]

IV. THE FEDERAL TRADE COMMISSION'S INITIATIVES

The Commission seeks to highlight the importance of information security using several approaches, including educating consumers and businesses, targeted law enforcement actions, international cooperation, and encouraging the private sector to develop and deploy information security technologies. Pursuant to its mandate under the Identity Theft Act, the Commission also facilitates information sharing among public and private entities to combat and help prevent identity theft.[12] Further, the Commission is currently working on a number of rulemakings implementing provisions of the Fair and Accurate Credit Transactions of 2003 ("FACT Act") that contain new and important measures to help reduce identity theft and facilitate identity theft

Exhibit 34

victims' recovery.[13]

A. Education and Outreach

Education is an essential element of the Commission's information security efforts. Our educational initiatives include public workshops to highlight emerging issues, consumer and business education to help identify risks to personal information and promote a "Culture of Security," and business education to promote compliance with relevant laws. For example, last year we held a two-session workshop, "Technologies for Protecting Personal Information: The Consumer and Business Experiences," to educate businesses, consumers, and ourselves about the challenges and possible technological solutions to securing electronic data.[14] In order to secure systems that contain personal information, panelists advised that businesses adopt a comprehensive risk-management strategy that incorporates four critical elements: people, policy, process, and technology.[15] Panelists also discussed a variety of recent initiatives in which industry is applying these principles. For example, companies have worked to reduce security flaws in software code, ship products in a more secure configuration, add new security features to products, and provide better security support, such as providing warnings and security patches, to their already-deployed products when security flaws appear.[16] In addition, panelists explored identity management tools and authentication issues as part of a risk-management plan.[17]

Our information security campaign also includes extensive outreach to businesses and consumers through our website, educational alerts, speeches, and participation in joint cybersecurity initiatives with other government agencies and private groups. The Commission devotes a portion of its website to educating businesses and consumers about security, and these

Exhibit 34

security-related pages are some of the most popular on our site.[18] The site includes guidance for businesses to reduce risks to their computer systems,[19] and tips for consumers on selecting online security products.[20] Our recent outreach efforts have also included cooperative ventures with the Department of Homeland Security and such organizations as the National Cyber Security Partnership and the National Cyber Security Alliance Stay Safe Online.[21]

B. Law Enforcement

The Commission's enforcement tools in information security matters derive generally from Section 5 of the FTC Act[22] and the Commission's Safeguards Rule.

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[23] To date, the Commission's security cases have been based on its authority to prevent deceptive practices.[24] These cases involved companies that made alleged express or implied promises that they would take appropriate steps to protect sensitive information obtained from consumers, but did not do so.[25] The complaints and consent orders in these cases reflect the principles discussed in Section III.A., above, and provide guidance to industry about implementing reasonable security procedures. In particular, the orders require, among other things, that the companies establish and maintain a comprehensive information security program that includes the basic elements necessary to ensure reasonable and appropriate security.

The Commission also has responsibility for enforcing its Safeguards Rule. The Rule requires a wide variety of non-bank financial institutions to implement comprehensive protections for customer information.[26] The Commission has issued guidance on the Rule[27] and met with a variety of trade associations and companies to promote compliance. Currently, Commission staff is conducting non-public investigations of compliance with the Rule.

Exhibit 34

Finally, an effective security program includes measures to ensure proper disposal of sensitive consumer information once it is no longer needed. Pursuant to the recently enacted FACT Act,[28] the Commission issued a proposed rule designed to reduce the risk of fraud or identity theft by ensuring that consumer reports, or information derived from consumer reports, are appropriately redacted or destroyed before being discarded.[29] The Commission anticipates the issuance of a final rule by the end of the year. Once the rule is in effect, it will provide an additional tool for use in the Commission's law enforcement efforts.

C. International Cooperation

In an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information, and the Commission has joined others in the global community to educate and establish a culture of security. For example, we played a leading role in developing and implementing the OECD Security Guidelines, assisted in developing and promoting a website dedicated to the global dissemination of information about the Guidelines,[30] and play an ongoing role in information privacy and security work undertaken by the OECD and the Asian Pacific Economic Cooperation ("APEC") forum.[31]

D. Encouraging the Development and Deployment of Information Security Technologies

The Commission also encourages the development and deployment of information security technologies that may help protect consumers from spam and "phishing" attacks. In its June 2004 Report to Congress concerning a possible National Do Not Email Registry, the Commission identified domain-level authentication as a promising technological development that would enable ISPs and other domain holders to better filter spam, and that would provide law enforcement with a potent tool for locating and identifying spammers.[32] Domain-level

Exhibit 34

authentication could also serve as a useful tool in preventing "phishing" spam and spam containing viruses from reaching consumers' inboxes. The Report concluded that the Commission could play an active role in spurring the market's development, testing, evaluation, and deployment of domain-level authentication systems. As a first step, the Report explained that the Commission, with other relevant government agencies, would hold an Email Authentication Summit in the Fall of 2004. The Commission and the Department of Commerce's National Institute of Standards and Technology will be hosting the Summit on November 9-10, 2004.

E. Assisting Identity Theft Victims

Through our efforts to promote information security and educate consumers, we hope to prevent identity theft before it occurs. When identity theft does occur, however, we also have an extensive program to help consumers who have been victimized. The program has three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; (2) maintaining and promoting the Identity Theft Data Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and (3) outreach and education to consumers, law enforcement, and private industry.

Victims may call the FTC through a toll-free hotline, 1-877-ID THEFT (438-4338), to receive telephone counseling from specially trained personnel. The phone counselors provide general information about identity theft and help guide victims through the steps needed to resolve the problems that result from the misuse of their identities.

The FTC also maintains the federal government's identity theft website,

Exhibit 34

www.consumer.gov/idtheft, which includes publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources. Consumers may file identity theft complaints on our secure online complaint form. These complaints are entered into the Identity Theft Data Clearinghouse and are used by law enforcement agencies to support their investigations.

The Commission also is currently working on a number of rulemakings implementing provisions of the FACT Act that provide new and important measures to facilitate identity theft victims' recovery. These include a national fraud alert system, which will eliminate the need for victims to contact each of the major credit reporting agencies separately,[33] and identity theft blocking, which will prevent fraudulent account information from being reported on consumer reports.[34] When fully implemented, these initiatives should help to reduce the incidence of identity theft, and help victims recover when the problem does occur. In addition, the Commission is consulting with the Treasury Department on its study, required by the FACT Act, of how the use of biometrics and similar authentication technologies to identify parties to a transaction might reduce the incidence of identity theft.[35]

V. CONCLUSION

Through a variety of education and enforcement initiatives, the FTC is working to ensure that all companies entrusted with personal information take reasonable steps to secure that information and minimize the risk that it may be misused. The agency has been and will continue to be vigilant in promoting a culture of security. We are educating consumers and businesses about the risks to personal information and the role they must play in enhancing security. We also will continue to assist victims of identity theft. In addition, the Commission

Exhibit 34

will continue to take action against companies that violate information security laws.

Exhibit 34

ENDNOTES

1. The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

2. The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act"). Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028). The Act did not confer on the FTC any additional law enforcement authority.

3. Social Security numbers in particular play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims.

4. For example, our 2003 Identity Theft Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf, showed that over 27 million individuals have been victims of identity theft, which may have occurred either offline or online, in the five years preceding the survey, including almost 10 million individuals in the year preceding the survey. The survey also showed that the average loss to businesses was $4800 per victim. Although in most cases, identity theft victims are not held liable for the fraudulent charges, they nonetheless suffer an average financial loss of $500, which reflects out-of-pocket expenses related to the efforts to dispute the frauds and repair their credit standing.

5. The Advisory Committee was comprised of forty e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates. Information about the Advisory Committee, including its charter, membership, meeting transcripts, and working papers, is available at http://www.ftc.gov/acoas/index.htm. The Advisory Committee submitted its Final Report to the Commission in May 2000. The Report recommended that companies undertake a security approach that is appropriate to the circumstances, and advised that a good security program includes: conducting a risk assessment; establishing and implementing a security system; managing policies and procedures based on the risk assessment; conducting periodic training for employees; conducting audits; conducting internal reviews; and conducting periodic reassessment of risk. *See Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security* (May 15, 2000), available at http://www.ftc.gov/acoas/papers/finalreport.htm.

6. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf. Pursuant to Section 501(b) of the Gramm-Leach-Bliley Act, the federal banking agencies have issued similar security guidelines that apply to the financial institutions they regulate. *See Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. Parts 30, app. B (OCC); 208, app. D-2 and 225, app. F (Board); 364, app. B (FDIC); 570, app. B (OTS).

Exhibit 34

7. In 2002, the OECD issued a set of nine voluntary principles for establishing a culture of security. The OECD principles are contained in a document entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." The principles address awareness, accountability, and action. They also recognize that security architecture and procedures should be appropriate for the kind of information collected and maintained and that good security is an ongoing process of assessing and addressing risks and vulnerabilities. *See* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

8. The FTC has developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, that provides advice on which law enforcement agency to contact, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, and information about contacting the FTC for assistance. The kit also provides FTC guidance regarding whether and how to notify consumers that there has been a breach. The information compromise kit is posted on our identity theft website, http://www.consumer.gov/idtheft and is also available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm.

9. Under certain state laws, companies may be required to notify consumers in the event of a breach. For example, the State of California requires consumer notification in the event of certain security breaches. The law, which went into effect July 1, 2003, requires a business or a State agency that maintains unencrypted computerized data that includes personal information to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is an individual's name plus one or more of the following: Social Security number, driver's license or state ID card number, or financial account numbers. *See* Cal. Civ. Code §§ 1798.29; 1798.82-1798.84.

10. The FTC's kit also includes a model letter for notifying individuals when that might be appropriate, such as when their names and Social Security numbers have been taken. Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

11. Prompt notification by businesses also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that individuals become victims, they can take action quickly to clear their records before any long-term damage is done.

12. The Federal Trade Commission maintains a database of identity theft complaints, and makes available and refers these complaints to criminal law enforcement agencies for investigation. Most identity theft cases are addressed best through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft, such as "pretexting" (tricking consumers or banks into revealing financial information) (*see, e.g.*, *FTC v. Corporate Marketing Solutions, Inc.*, Civ. No. 02-1256-PHX (RCB) (D. Ariz. Feb. 3, 2003) (final order)) or "phishing" (using spam email that looks like it comes from a legitimate website to deceive consumers into providing account or other

Exhibit 34

sensitive information) (*see, e.g., FTC v. M.M.*, Civ. No. 04-2086 (E.D.N.Y. May 18, 2004) (final order)). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. *Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam* (Jan. 16, 2003) (at http://www.ftc.gov/opa/2003/01/idpfinal.htm).

13. Pub. L. No. 108-159 (2003).

14. The FTC staff released a short staff summary of the findings from the workshop, which is available at http://www.ftc.gov/bcp/workshops/technology/index.html.

15. *See* Staff Workshop Report: Technologies for Protecting Personal Information, at 2-3.

16. *Id.* at 4-5.

17. In particular, the National Academies of Science and the Center for Democracy and Technology discussed the strengths and weaknesses of certain identity systems, and the distinctions between identification, authentication, and authorization.

18. *See* http://www.ftc.gov/infosecurity.

19. *Security Check: Reducing Risks to Your Computer Systems*, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

20. *Detect, Protect, Disinfect: Consumers On Line Face Wide Choices in Security Products*, available at http://www.ftc.gov/bcp/conline/pubs/alerts/idsalrt.htm.

21. These include the consumer education website, www.staysafeonline.info.

22. 15 U.S.C. § 45.

23. 15 U.S.C. § 45(a)(1).

24. The Commission and the courts have defined a deceptive practice as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances. Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), *reprinted* in appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (setting forth the Commission's Deception Policy Statement). The Commission also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. 15 U.S.C. § 45(n). The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with "phishing." *See FTC v. Hill*, Civ. No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

Exhibit 34

25. *See MTS, Inc. d/b/a Tower Records/Books/Video*, FTC Dkt. No. C-4110 (June 2, 2004); *Guess?, Inc.*, FTC Dkt. No. C-4091 (August 5, 2003); *Microsoft Corp.*, FTC Dkt. No. C-4069 (Dec. 24, 2002); *Eli Lilly, Inc.*, FTC Dkt. No. C-4047 (May 10, 2002). The complaints and decisions and orders in these cases are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

26. The Rule requires covered financial institutions within the Commission's jurisdiction to develop a written information security plan to protect customer information that is reasonable in light of a company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must include certain basic elements, including: (1) designating one or more employees to coordinate the safeguards; (2) identifying and assessing the risks to customer information in each relevant area of the company's operation, and evaluating the effectiveness of the current safeguards for controlling these risks; (3) designing and implementing a safeguards program, and regularly monitoring and testing it; (4) hiring appropriate service providers and contracting with them to implement safeguards; and (5) evaluating and adjusting the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

27. *Financial Institutions and Customer Data: Complying with the Safeguards Rule*, available at http://www.ftc.gove/bcp/conline/pubs/buspubs/safeguards.htm.

28. The FACT Act amends the Fair Credit Reporting Act in a number of ways, including the addition of a number of provisions intended to combat consumer fraud and related crimes, including identity theft.

29. *See* Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21,388 (2004) (to be codified at 16 C.F.R. Part 682), available at http://www.regulations.gov/fredpdfs/04-08904.pdf. To help prevent identity theft, the FACT Act also directs the Commission to issue a "red flags" rule. *See* Pub. L. No. 108-396, § 157 (2003). The rule will help creditors analyze identity theft patterns and practices so that they can take appropriate action to prevent this crime.

30. *See* http://www.oecd.org/sti/cultureofsecurity.

31. The APEC Electronic Commerce Steering Group ("ECSG") promotes awareness and responsibility for cybersecurity among small and medium-sized businesses that interact with consumers. Commission staff participated in APEC workshop and business education efforts this past year and will remain actively engaged in this work for the foreseeable future.

32. The Commission's National Do Not Email Registry Report is available at: http://www.ftc.gov/reports/dneregistry/report.pdf.

33. Pub. L. No. 108-396, § 112 (2003).

Exhibit 34

34. Pub. L. No. 108-396, § 152 (2003)

35. Pub. L. No. 108-396, § 157 (2003)

Exhibit 34

EXHIBIT 35

072-3055

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **William E. Kovacic, Chairman**
Pamela Jones Harbour
Jon Leibowitz
J. Thomas Rosch

In the Matter of	)	
	)	
THE TJX COMPANIES, INC.	)	**DOCKET NO. C-4227**
a corporation.	)	
	)	

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

Exhibit 35

1. Respondent The TJX Companies, Inc. is a Delaware corporation with its principal office or place of business at 770 Cochituate Road, Framingham, Massachusetts, 01701.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

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 or debit card information, including card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and check number; (h) a driver's license, military, or state identification number; (i) 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 (j) any information that is combined with any of (a) through (i) above.

2. Unless otherwise specified, "respondent" shall mean The TJX Companies, 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:

Exhibit 35

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 development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by sub-Part 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, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

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

B. explain 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;

Exhibit 35

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

D. certify 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 has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies 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 initial 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 Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such 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 having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel

Exhibit 35

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 the 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 Part 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 eighty (180) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on July 29, 2028, 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 Part 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 Part.

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 Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and

Exhibit 35

the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: July 29, 2008

Exhibit 35