

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

**RESPONDENT’S MOTION TO LIMIT EVIDENCE TO THE
TIME FRAME OF THE EXPERT REPORT AND OPINION**

Respondent LabMD, Inc. (“LabMD”) moves this Court for an Order limiting the relevant time period concerning the adequacy of LabMD’s data security protocols to January 2005 through July 2010. The FTC’s expert witness, Dr. Raquel Hill, testified that her opinion on the adequacy of LabMD’s security protocols only ranged from January 2005 to July of 2010. Hill Depo., dated Apr. 18, 2014, attached hereto in relevant part as Exh. 1, at 138. For reasons explained more fully below, the FTC should not be permitted to present evidence regarding the adequacy of LabMD’s security protocols beyond the time frame set by its expert.

I. LAW AND ARGUMENT

Commission Rule of Practice 3.31A, 16 C.F.R. § 3.31A, provides that “[t]he parties shall serve each other with a list of experts they intend to call as witnesses at the hearing. . .” 16 C.F.R. § 3.31A(a). This rule also generally requires that this disclosure be accompanied by a written report containing:

- (i) a complete statement of all opinions to be expressed and the basis and reasons therefor;
- (ii) the data, materials, or other information considered by the witness in forming the opinions;
- (iii) any exhibits to be used as a summary of or support for the opinions;

- (iv) the qualifications of the witness, including a list of all publications authored by the witness within the preceding 10 years;
- (v) the compensation to be paid for the study and testimony; and a listing of any other cases in which the witness has testified as an expert at trial or by deposition within the preceding 4 years.

16 C.F.R. § 3.31A(c).

“The purpose of [Commission Rule of Practice 3.31A] is to prevent unfair surprise at trial and to permit the opposing party to prepare rebuttal reports, to depose the expert in advance of trial, and to prepare for depositions and cross-examinations at trial.” *Minebea Co., Ltd. v. Papst*, 231 F.R.D. 3, 5-6 (D.D.C. 2005); *see also Muldrow ex rel. Estate of Muldrow v. Re-Direct, Inc.*, 493 F.3d 160, 167, 377 U.S. App. D.C. 187 (D.C. Cir. 2007) (quoting *Sylla-Sawdon v. Uniroyal Goodrich Tire Co.*, 47 F.3d 277, 284 (8th Cir. 1995)).¹

In line with that purpose, Fed. R. Civ. P. 37 provides that a party that fails to disclose information required by Rule 26(a) “is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless.” Fed. R. Civ. P. 37 (c)(1).

Additionally, the Scheduling Order prohibits fact witnesses from providing expert opinion, Scheduling Order at 18, and Fed. R. Evid. 701 prohibits lay witnesses from offering opinions based on specialized knowledge. *See also Basic Research*, No. 9318, 2006 FTC LEXIS 5, *9 (Jan. 10, 2006) (Order on Complaint Counsel's Motion In Limine) (if the witnesses "perform[ed] the tests or have firsthand knowledge of the tests upon which Respondents relied for substantiation for their products, they may testify, but only to the extent of their personal knowledge of how the conclusions were drawn"). Arguably, this rule is intended to eliminate the

¹ Commission Rule of Practice 16 3.31A directly mirrors Fed. R. Civ. P. 26(a)(2). Federal case law is instructive here as this Court has stated that “. . . since many adjudicative rules are derived from the Federal Rules of Civil Procedure, the latter may be consulted for guidance and interpretation of Commission Rules . . .” Federal Trade Commission Operating Manual Ch. 10.6.

risk that the reliability requirements set forth in Commission Rule of Practice 3.43(b) will be “evaded through the simple expedient of proffering an expert in lay witness clothing.” *Bell v. Gonzales*, 2005 U.S. Dist. LEXIS 37879, at *41 (D.D.C. Dec. 23, 2005) *citing* Fed. R. Evid. 701 advisory committee notes.

i. The FTC’s Expert Opinion Regarding the Adequacy of LabMD’s data Security is Limited to the Timeframe of January 2005 to July 2010

Based upon Dr. Hill’s expert report and deposition testimony, neither she nor any other FTC witness should be permitted to offer expert opinion, lay opinion, or introduce additional evidence concerning the adequacy of LabMD’s security protocols *after July 2010*. Dr. Hill did not provide an opinion on LabMD’s security protocols for any time after July 2010. Her deposition makes this very clear:

Q: Now, Dr. Hill, you defined the relevant time period as 2005 through 2010; is that correct?

A: Yes. Well, from January 2005, and I think we have it -- it's not all of 2010.

Q: You’re right.

A: I think its July of 2010...
Hill Depo., Exh. 1, at 138.

...

Q: Is it fair to say, then, that you have not expressed any opinion with regard to the adequacy of LabMD's data security after July of 2010?

A: I haven't expressed any opinion after July of 2010.
Id. at 140

To be sure, Commission Rule of Practice 3.31A does not limit an expert’s testimony simply to reading her report. *In re POM Wonderful LLC*, 2011 FTC LEXIS 77 (F.T.C. May 5, 2011). However, LabMD is not requesting an unreasonable restriction on Dr. Hill’s testimony—

only that it is limited to the time frame that she so clearly expresses in her report and deposition testimony.

Dr. Hill testifies at length about data security, and in doing so demonstrates the specialized knowledge and scientific nature of the subject matter. As such, Dr. Hill should be precluded from testifying as to the adequacy of LabMD's data security after July of 2010 because she did not provide an opinion on that issue in her report or in her deposition.

The deadline for the FTC to supply or supplement its expert reports has passed; therefore, this Court may limit the FTC's case to the opinions disclosed in its expert report in order to prevent the FTC from "sandbagging" LabMD with new evidence. *Ebewo v. Martinez*, 309 F. Supp. 2d 600 (S.D.N.Y. 2004). To allow such testimony or the introduction of evidence beyond the time frame established by Dr. Hill's report would not permit LabMD the opportunity to adequately rebut or cross examine Dr. Hill's newly formed opinions as required under the rule.

ii. Lay Witnesses Cannot Testify to the Adequacy of LabMD's Security Protocols After July 2010

Properly qualified expert witnesses may testify regarding their specialized knowledge in a given field if it "would assist the trier of fact to understand the evidence or to determine a fact in issue." See *In the Matter of South Carolina State Board of Dentistry*, 2004 FTC LEXIS 134 (F.T.C. Aug. 9, 2004)(citing Fed.R.Evid. 702). The FTC seeks to present evidence concerning the adequacy of LabMD's data security after July 2010. The only purpose for the submission of this evidence is for the trier of fact to make a determination as to the adequacy of LabMD's data security based upon that evidence. Expert testimony is relied upon when it can offer something "beyond the understanding and experience of the average citizen." *United States v. Paul*, 175 F.3d 906, 911 (11th Cir. Ga. 1999) quoting *United States v. Rouco*, 765 F.2d 983, 995 (11th Cir. 1985); see also *United States v. Burchfield*, 719 F.2d 356 (11th Cir. 1983) (explaining that expert

testimony is admissible where it is “the kind that enlightens and informs lay persons without expertise in a specialized field”). Here, the adequacy of data security is a specialized field that is sufficiently complex such that the untrained layman is unable to intelligently determine the issue without guidance from an expert.

While lay witnesses may testify or introduce evidence regarding what security protocols LabMD had in place after July of 2010, they may not give opinion testimony as to whether it was adequate, nor do they possess the specialized knowledge to assist this Court in making that determination. Moreover, as discussed above these lay witnesses have not been designated as expert witnesses nor met the procedural requirements of 16 C.F.R. § 3.31A(a). Thus, the presentation of such evidence would be a waste of the Court’s time. Appendix B of Dr. Hill’s report lists an abundance of documentation including deposition testimony of lay witnesses which she considered in forming her opinion. If after her expert review, Dr. Hill did not conclude that LabMD’s data security was inadequate post July 2010, why should this Court as trier of fact attempt to draw some different conclusion from the same evidence? *See* Report of Dr. Raquel Hill and Appendix B thereof, attached hereto as Exh. 2.

II. CONCLUSION

Based upon the foregoing, LabMD respectfully requests this Court for an Order limiting the evidence to be presented at trial regarding LabMD’s data security to the time period of January 2005 to July 2010 as set forth in the report of the FTC’s expert on data security, Dr. Raquel Hill.

Respectfully submitted,

/s/ William A. Sherman, II
William A. Sherman, II
Reed D. Rubinstein
Sunni R. Harris
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9100
Fax: 202.372.9141

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

Dated: May 2, 2014

**STATEMENT REGARDING MEET AND CONFER PURSUANT TO 16 C.F.R. § 3.22(g)
AND ADDITIONAL PROVISION 4 OF THE SCHEDULING ORDER**

Respondent respectfully submits this Statement, pursuant to F.T.C. Rule 3.22(g) and Additional Provision 4 of the Scheduling Order. Prior to filing the attached Motion to Compel Testimony, Respondent met and conferred with Complaint Counsel, in an effort in good faith to resolve by agreement the issues raised by the motion and has been unable to reach an agreement. Respondent Counsel William Sherman and Kent Huntington engaged in a meet-and-confer with Complaint Counsel Laura VanDruff, Alain Sheer, Maggie Lassack, and Megan Cox on Wednesday, April 30, 2014, at approximately 10:30 am, regarding Complaint Counsel's refusal to limit the relevant time frame to January 2005 through July 2010 as limited by their expert Dr. Raquel Hill's report. Counsel for the FTC indicated that they intended to present evidence concerning the adequacy of LabMD's data security post July 2010. Despite good faith efforts, an agreement was unable to be reached.

Dated: May 2, 2014

Respectfully,

/s/ William A. Sherman, II
William A. Sherman, II, Esq.

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

| | |
|--------------------|-----------------|
| _____) | |
| In the Matter of) | DOCKET NO. 9357 |
|) | |
| LabMD, Inc.,) | |
| a corporation.) | |
|) | |
| _____) | |

[PROPOSED] ORDER GRANTING LabMD, Inc.’s MOTION TO LIMIT EVIDENCE TO THE SCOPE OF THE EXPERT REPORT AND OPINION

Upon consideration of Respondent LabMD, Inc.’s Motion to Limit Evidence to the Scope of the Expert Report and Opinion, and in consideration of the entire Record in this matter, IT IS HEREBY ORDERED that LabMD, Inc.’s Motion is GRANTED.

ORDERED:

D. Michael Chappell
Chief Administrative Law Judge

Date:

CERTIFICATE OF SERVICE

I hereby certify that on May 2, 2014, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

I also certify that on May 2, 2014, 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 on May 2, 2014, I delivered via electronic mail and first-class mail a copy of the foregoing document to:

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

CERTIFICATE OF ELECTRONIC FILING

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

Dated: May 2, 2014

By: /s/ William A. Sherman, II
William A. Sherman, II

EXHIBIT 1

**Transcript of the Testimony of Raquel Hill
Dated: April 18, 2014**

Transcript of the Testimony of **Raquel Hill**

Date: April 18, 2014

Case: In The Matter of: LabMD, Inc.



Ace-Federal Reporters, Inc.
Phone: 202-347-3700
Fax: 202-737-3638
Email: info@acefederal.com
Internet: www.acefederal.com

Page 134

1 this policy?"

2 Answer: "Yes."

3 Does that change your mind as to whether or not

4 at least Mr. Maire thought and testified that these

5 policies were in place in the 2007-2008 time frame?

6 A So what it does, it tells me that this -- this

7 audit and security operations internet connectivity

8 policy was in place, and that he was one of the people

9 who worked to enforce it.

10 Q My question is: Did you take those facts that

11 you have just mentioned into consideration while drawing

12 your conclusions about the adequacy of LabMD's data

13 security?

14 A Yes.

15 Q If you look at -- again, we're still in RX-5.

16 If you could turn to the page that's Bates numbered --

17 I'll let you get there.

18 A Yeah, I'm looking at it. I just have different

19 parts of it.

20 Q The page is Bates numbered 3150.

21 A Okay.

22 Q Did you -- I think you've already testified --

Page 136

1 Bates numbered FTC-LabMD-003153, that is the "monitor

2 security software settings and operating systems updates

3 policy." Do you see that?

4 A Yes.

5 Q Did you take this policy into consideration when

6 you were drawing your conclusions and opinions with

7 regard to LabMD's data security?

8 A Yes.

9 Q Did you also take into -- I'm sorry, if we could

10 turn to RX-6, Mr. Maire's excerpt.

11 If you look at page 24 of his excerpt at line 7,

12 it indicates: "I want to move to the last policy that

13 you recalled which is on CX-6, page 13, Bates number

14 FTC-LabMD-003153, and this is the monitor security

15 software settings and operating system updates policy.

16 Please take a moment to look at this policy and let me

17 know if it accurately describes the practices at LabMD

18 during your tenure."

19 The answer is: "Yes."

20 The question: "Did you have a role in enforcing

21 this policy?"

22 The answer is: "Yes."

Page 135

1 well, let me just ask you. Did you review the data

2 backup policy as reflected on Bates number

3 FTC-LabMD-003150, while you were considering and

4 formulating your opinions with regard to LabMD's data

5 security?

6 A Yes.

7 Q If you look at page 22 of Mr. Maire's deposition

8 excerpts, line 17: Question: For the data backup policy

9 which is CX-6, page ten, with the Bates number of

10 FTC-LabMD-003150, will you take a look at this policy and

11 tell me if it accurately describes LabMD's practices

12 during your tenure?"

13 His answer is: "Yes."

14 And again: "Did you participate during your

15 tenure at LabMD in enforcing this data backup policy?"

16 The answer is: "Yes."

17 In formulating your opinion and conclusions with

18 regard to LabMD's data security policy, did you consider

19 the fact that this data backup policy was in effect as

20 early as 2007?

21 A Yes.

22 Q If we go back to RX-5, again, and go to the page

Page 137

1 Again, in drawing your conclusions and opinions

2 with regard to LabMD's data security, did you take into

3 consideration that the monitor security software settings

4 and operating systems update policy was in effect as

5 early as 2007?

6 A This particular policy, as stated. There are

7 other deposition testimonies that specifically that

8 automatic updates were disabled.

9 So, generally, I took all of these policies.

10 You know, whether I thought they were in writing or not,

11 I took these as the policies that they were following.

12 So on all the ones in the policy manual, that these were

13 their policies.

14 Now, whether they were being followed or not,

15 is, you know, one thing that I looked across the

16 depositions to determine. And whether I thought they

17 were, you know, complete or comprehensive, that was

18 another thing when considering the policies.

19 Q As we were going through the seven principles

20 and discussing policies earlier, we did talk about

21 passwords and you indicated that based on your review of

22 the documentation, you were aware that passwords were

In The Matter of: LabMD, Inc.

Page 138

1 required; is that correct?
 2 A Yes.
 3 Q You, however, indicated that you did not believe
 4 that the policy was adequate because there was no mention
 5 of the acceptable minimum length of a password or the
 6 lifetime of the password or the password history; is that
 7 correct?
 8 A Yes. And other characteristics of strength of
 9 passwords, yes.
 10 Q Now, Dr. Hill, you defined the relevant time
 11 period as 2005 through 2010; is that correct?
 12 A Yes. Well, from January 2005, and I think we
 13 have it -- it's not all of 2010.
 14 Q You're right.
 15 A I think it's July of 2010, but it's somewhere
 16 here in the document. Yes, it's on paragraph 4, I'm
 17 not -- and page 1 of my document.
 18 Q And I asked you when the deposition began
 19 whether you had received additional information or
 20 reviewed additional documentation which would cause you
 21 to anticipate having to amend your report, and your
 22 counsel added that you still reserved the right to do so,

Page 139

1 but your answer was that you did not anticipate based on
 2 the documents that you have seen to date having to amend
 3 your report; is that correct?
 4 A Yes.
 5 Q And that would include the relevant time period
 6 as well; is that correct?
 7 MS. LASSACK: I just want to clarify, that's
 8 for Professor Hill's analysis --
 9 MR. SHERMAN: Yes.
 10 MS. LASSACK: -- when you are referring to
 11 relevant time period. Okay, I just wanted to clarify
 12 that.
 13 A So based on the documents that I -- your
 14 question is based on the documents that I've reviewed and
 15 that --
 16 BY MR. SHERMAN:
 17 Q Thus far.
 18 A And that I've reviewed and not any that I may
 19 receive, that's what you're talking about, right?
 20 Q That's correct.
 21 A Okay, yes. Based on the documents that I have
 22 reviewed, no, I -- I see no reason to change the relevant

Page 140

1 time period.
 2 Q Is it fair to say, then, that you have not
 3 expressed any opinion with regard do the adequacy of
 4 LabMD's data security after July of 2010?
 5 A I haven't expressed any opinion after July of
 6 2010.
 7 Q Let's look at RX-3, which I think you already
 8 have.
 9 A Yes.
 10 Q Which is the employee handbook.
 11 A I'm sorry.
 12 Q Don't apologize. This is not a normal process.
 13 Dr. Hill, if you could to turn to page 5 of
 14 RX-3, which is the employee handbook. Is this a document
 15 that you reviewed in formulating your conclusions and
 16 opinions with regard to LabMD's data security?
 17 A Yes.
 18 Q On page 5, the last two paragraphs have to deal
 19 with confidentiality and trade secrets.
 20 Do you see that?
 21 A Yes.
 22 Q And it indicates that, "It is one of your most

Page 141

1 serious responsibilities that you in no way reveal or
 2 divulge any such information and that you use in information
 3 only in the performance of your duties, as certain
 4 information could be used by competitors. Violation of
 5 this may subject you to immediate termination."
 6 Do you see that?
 7 A If you would just give me a moment, I'm just
 8 reading. I was listening.
 9 Yes.
 10 Q The next paragraph indicates that, "Employees
 11 who need to remove LabMD property, equipment, records, or
 12 information from the premises must have proper
 13 authorization."
 14 Do you see that?
 15 A Yes.
 16 Q Now, while these statements do not directly
 17 mention data security, and they appear in the employee
 18 handbook, would these qualify, in your opinion, as
 19 policies of the company?
 20 A I think that they are policies of the company.
 21 Q And so if you turn the page, the next page is
 22 page 6, same document, it talks about, "The Health

Page 142

1 Insurance Portability and Administrative Act (HIPAA) of
 2 1993 made it illegal for any person in health care to
 3 share an individual's protected health care information
 4 with anyone other than for the specific reasons of
 5 treatment, payment or health care operations."
 6 Do you see that?
 7 A Yes.
 8 Q Do you consider that, even though it's in the
 9 employee handbook, to be a policy of the company?
 10 A Yes.
 11 Q And would it be beneficial, then, for employees
 12 to have read this with regard to the importance that the
 13 company assigned to protecting health care information?
 14 A Yes.
 15 Q If you will turn to the next page, there is a
 16 section on "Personal Mail, E-mail and Phone Calls."
 17 Do you see that?
 18 A Yes.
 19 Q The second paragraph indicates that, "Personal
 20 internet or e-mail usage in the office is prohibited.
 21 This policy stands at all times, even when an employee is
 22 on a lunch period. Computers in the office are property

Page 143

1 of LabMD and should only be used for company related
 2 reasons."
 3 Did I read that correctly?
 4 A Yes.
 5 Q Do you consider that to be a policy that would
 6 have had an impact on an employee's understanding of the
 7 use of computers of LabMD's computers?
 8 A Yes.
 9 Q Would you consider that policy as being helpful
 10 in terms of the importance -- communicating to employees
 11 the importance that LabMD placed on the security of its
 12 information?
 13 A I don't know whether this policy is -- you know,
 14 was specifically written, you know, for a data security
 15 purpose. It's reasonable to say it's, you know, for a
 16 functional business purpose, and so I don't know it's
 17 a --
 18 Q Let me ask it a different way. Would this
 19 policy, as written, be beneficial to a company with
 20 regard to its efforts to protect sensitive information?
 21 A I think so.
 22 Q Two paragraphs down, it says, "You will be

Page 144

1 reprimanded for failure to comply with this office
 2 policy."
 3 Do you consider that an enforcement mechanism
 4 with regard to requiring employees to adhere to the
 5 written policies of the company?
 6 A We've talked about enforcement mechanisms before
 7 and I go back to my original testimony regarding
 8 enforcement mechanisms. There is a technical enforcement
 9 mechanism, so when there is no other -- if there's not a
 10 technical mean for enforcing it, then a written policy,
 11 you know, explaining the repercussions of violating the
 12 policy. You know, I guess if that's all you have, that's
 13 all that you do. But if there's a technical mean for
 14 enforcing it, then that is the mean that's going to be
 15 more effective.
 16 Q If you will turn, then, to page 12 of that
 17 document, there is a section at the bottom of the page
 18 called, "LabMD Discipline."
 19 Do you see that section?
 20 A Yes.
 21 Q It reads: It is the policy of LabMD that any
 22 conduct which is -- which in its view interferes with or

Page 145

1 adversely affects employment, is sufficient to impose
 2 disciplinary action ranging from an oral warning to
 3 immediate termination. Factors that may be considered in
 4 ascertaining the appropriate discipline include, but are
 5 not limited to:"
 6 And I'll ask that you turn to the next page, as
 7 it goes down a list of things.
 8 On page 13, do you see near the bottom of the
 9 list, "Unauthorized disclosure of any confidential LabMD
 10 information"?
 11 A And when you say "information," are you -- are
 12 you referring to materials? Is that it?
 13 Q I'm just reading what's said. I can assume what
 14 the author means, but I'm just reading what's there on
 15 the bullet points.
 16 A I was reading the wrong "unauthorized."
 17 Q That's okay.
 18 A Sorry.
 19 Q And it --
 20 A Yes.
 21 Q And it also says "Removing or borrowing LabMD
 22 property without proper authorization" and it goes on

EXHIBIT 2

**Expert Report of Raquel Hill, Ph.D.
Dated: March 18, 2014**

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.)

EXPERT REPORT OF RAQUEL HILL, PH.D.

TABLE OF CONTENTS

| | | |
|-------|---|----|
| I. | Introduction..... | 1 |
| II. | Summary of Experience and Qualifications | 2 |
| III. | Overview of Network Security Principles | 4 |
| | A. Background: Computer Networks | 4 |
| | B. Defense in Depth..... | 8 |
| | C. Principles for Assessing and Securing a Network | 11 |
| IV. | LabMD’s Network During the Relevant Time Period..... | 13 |
| V. | Scope of Opinions..... | 16 |
| VI. | Materials Considered in Forming Opinions..... | 17 |
| VII. | Summary of Opinions | 18 |
| VIII. | Opinions | 19 |
| | A. Comprehensive Information Security Program – Complaint ¶ 10(a)..... | 19 |
| | B. Risk Assessment – Complaint ¶ 10(b)..... | 24 |
| | C. Access to Information Not Needed to Perform Jobs – Complaint ¶10(c) | 30 |
| | D. Information Security Training – Complaint ¶10(d)..... | 34 |
| | E. Use of Authentication Related Security Measures – Complaint ¶10(e) | 36 |
| | F. Maintenance and Updating of Operating Systems– Complaint ¶10(f)..... | 38 |
| | G. Prevention and Detection of Unauthorized Access – Complaint ¶10(g) | 41 |
| IX. | Conclusion | 46 |

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 Information¹ 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 a natural person including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. See Complaint Counsel's February 19, 2014 Requests for Admission to LabMD, p. 2.

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

II. Summary of Experience and Qualifications

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

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

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

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

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

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

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

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

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

III. Overview of Network Security Principles

A. Background: Computer Networks

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

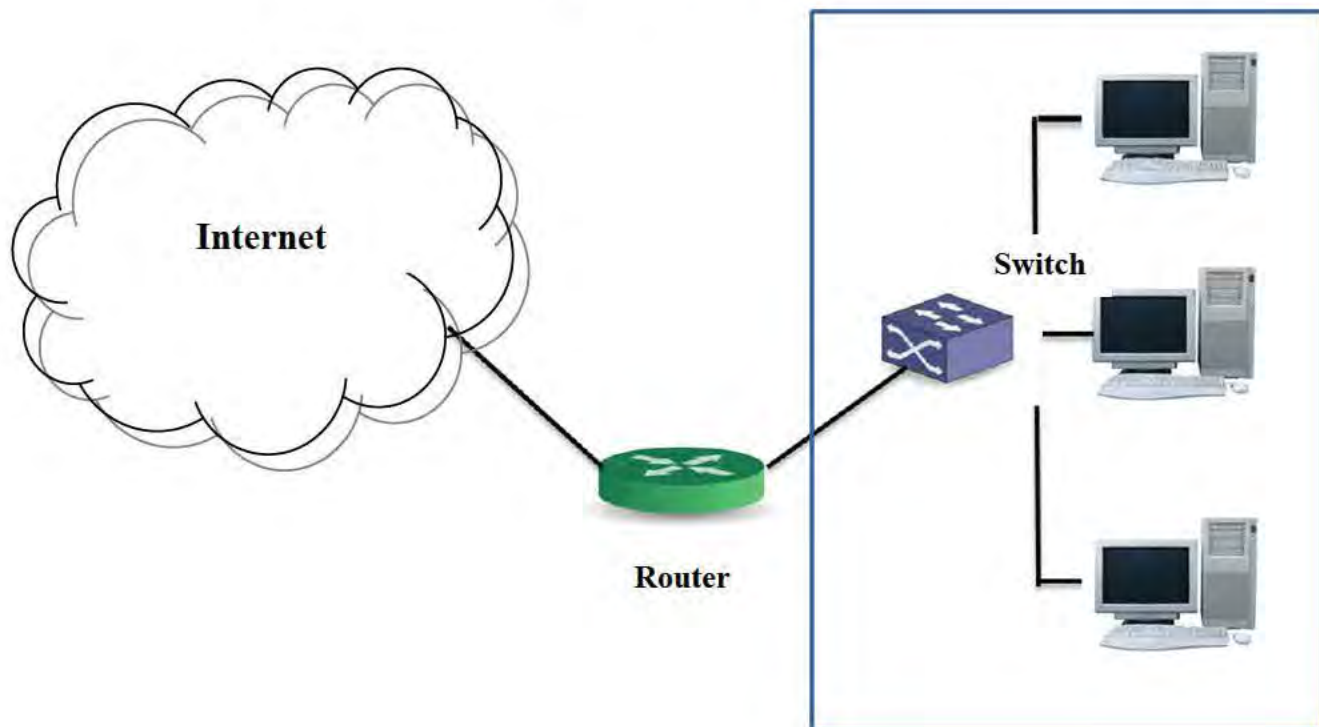
14. Computers use network interface cards (NIC) to connect to a network, and each NIC has a unique media access control (MAC) address. Each computer within a network is therefore uniquely identified by the MAC address of the computer's NIC. A computer's MAC address is not known outside of a computer's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

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

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

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

Figure 1: Connecting to the Internet



i. Network Addresses and Ports

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

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

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

ii. Firewalls and Intrusion Detection Systems

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

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

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

iii. Authentication and Access Control

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

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

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

B. Defense in Depth

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

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

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

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

- a. **Internet Connection Layer:** At this layer, we cannot prevent software from being installed on a workstation or server, but we can restrict the type of traffic that flows into the network. Therefore, even if unauthorized software has been inadvertently installed on a workstation/server, mechanisms could be used to render the application

ineffective. Recall that port numbers map to specific applications, and that firewalls can be configured to restrict the types of application traffic that is allowed into the network, by dropping any data that contains an unauthorized port number. Thus, to illustrate the concept of defense in depth, a first line of defense to prevent use of unauthorized applications is to configure a firewall to close all ports at the gateway router except those that are used by authorized applications. Other mechanisms besides firewalls could be deployed at this layer as well, such as an IDS.²

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

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

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

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

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

C. Principles for Assessing and Securing a Network

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

- a. **Don't Keep What You Don't Need:** The first principle recognizes that maintaining sensitive information that is not needed creates an unnecessary risk.
- b. **Patch:** A most basic principle is to Patch, meaning to apply updates to fix all known or reasonably foreseeable security vulnerabilities and flaws.
- c. **Ports:** The third principle concerns Ports. As previously stated, applications communicate via ports. There are well-known ports for well-known applications. For example, a web server listens for incoming connections on Ports 80 and 443. All unused ports should be closed.
- d. **Policies:** Policies are processes and procedures that are put in place to satisfy an organization's security requirements. Examples of policies would include the following:
 - **Data Access** – Limit data access to persons with a need for the data.
 - **Passwords** – Policies regarding passwords should contain rules about the following:
 - Acceptable minimum length.
 - Lifetime of a password.
 - The lifetime of a password is often related to the sensitivity of the information that the user accesses, the greater the sensitivity, the shorter the password's lifetime.
 - Password history.

- Passwords to avoid.
 - If you are a big sports fan, don't use a password that is related to your favorite team.
 - Avoid personal data such as spouse's name, children's name, pet's name, and birthdays.
- **Backups** – Backup data on a regular basis to be able to restore it because data is more valuable than the computer.
 - Encrypt backups.
 - Keep data in a secure location.
 - Limit access to backups.
- e. **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.

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

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

IV. LabMD's Network During the Relevant Time Period

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

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

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

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

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

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

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

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

39. LabMD's network included a number of servers that hosted applications, including back-up, email, webserver, database, laboratory, and billing applications. Some of these servers hosted multiple applications and also stored Personal Information. For example, one server hosted billing and mail applications³

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

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

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

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

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

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

⁴ See FTC-LABMD-3755 (CX0152).

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

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

because, for example, a computer with a copy might be turned off when the search occurs.

Security professionals and others have warned about this risk since at least 2005.

V. Scope of Opinions

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

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

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

that the systems would 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,

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

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

VII. Summary of Opinions

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

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

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

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

VIII. Opinions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

b. Although LabMD contends that the policies set forth in LabMD's Policy Manual¹¹ were in place in 2007 and 2008, there is no documentation demonstrating that those policies were in place, and if they were in place, at least some of those policies were not being enforced. For example:

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

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

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

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

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

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

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

B. Risk Assessment – Complaint ¶ 10(b)

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

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

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

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

¹⁵ This vulnerability is discussed in Paragraph 100, below.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

cost of having penetration tests is modest: the penetration test LabMD had performed in 2010 by ProviDyn, an IT service provider, cost \$450.²³

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

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

74. The process for choosing reasonable and appropriate measures to address risks discovered through risk assessment is well-known and understood among IT practitioners and businesses. Guidelines on how to select reasonable and appropriate security measures have been freely available for years. NIST, for example, published a standard that explained the process in 2002.²⁵ In 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central

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

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

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

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

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

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

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

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

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

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

²⁷ See, for example, Paragraph 71, above.

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

i. Whether LabMD Maintained More Personal Information than Necessary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

91. Record evidence shows that LabMD did not adequately train employees to safeguard Personal Information or provide appropriate opportunities for its IT employees to receive formalized security related training about evolving threats and how to protect against them.³¹

This resulted in gaps in their knowledge and a creation of security processes that were reactive, incomplete, ad hoc, and ineffective. For example, prior to 2010:

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

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

- a. Penetration testing was never done;³²
 - b. Software with known flaws was not updated on servers that contained Personal Information;³³
 - c. Firewalls were disabled on servers that contained Personal Information;³⁴
 - d. Servers executed software that was no longer supported by vendors, including operating system and antivirus software;³⁵
 - e. There was no uniform policy requiring strong passwords or expiration of passwords;³⁶
 - f. Personal Information was transmitted and stored in an unencrypted format;³⁷
 - g. At least some employees were given administrative access accounts and were able to download and install software without restriction, etc.³⁸
92. LabMD could have adequately trained employees to safeguard Personal Information at relatively low cost.³⁹

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- LabMD billing employee Sandra Brown testified that she used the same username, sbrown, and password, labmd, to access her LabMD computer on site and remotely from 2006 to 2013.⁴⁰

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

- LabMD created weak passwords for the nurses' user accounts that were created on the computers that it placed in its physician clients' offices. The typical password included the nurse's initials.⁴¹
- Although the Windows operating systems that LabMD used provided a centralized scheme to manage passwords, LabMD did not use that functionality.⁴²
- Requiring two-factor authentication for remote users would have implemented a defense in depth strategy and could have compensated for LabMD's failure to require the use of strong passwords. LabMD did not use two-factor authentication.⁴³

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

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

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

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

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

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

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

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

98. Researchers have found that experienced programmers introduce 1 bug per every 10 lines of code that they write.⁴⁵ Therefore, for a program like Windows Server 2003⁴⁶ that has 50 million lines of code, you can expect approximately 5 million software bugs to be introduced while the software is being developed. While many of the bugs will be detected and fixed during system testing, not all bugs will be identified before the product is shipped. In addition, code that was added to fix a problem may also introduce new bugs.

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

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

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

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

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

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

b. Record evidence shows that LabMD did not apply software updates in accordance with the policies it claims were in place during the Relevant Time Period⁴⁸ 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 shows that the LabMD Labnet server was running a version of Veritas Backup software that was configured with the default administrative password. This vulnerability had a Level 5 (Urgent Risk) rating, which means that an attacker can compromise the entire host. This problem was detected in 2010, and the corresponding solution was available as early as August 15, 2005. The Veritas software on the Labnet server also contained a Level 4 (Critical) buffer overflow vulnerability that would allow an attacker to execute arbitrary code on the remote host.⁵¹ This problem was also detected

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- a. Employees should be given non-administrative accounts on workstations, thereby preventing them from installing software. Windows includes the functionality to enforce this policy in its operating systems package. This is a cost free measure.
- b. Backups of Personal Information should be stored on devices that are isolated from other employee activities. An employee's workflow may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, unauthorized changes, etc. Therefore, backups of Personal Information should not be stored on multi-purpose employee workstations. Enforcing such a policy could be cost-free, if the organization designated an existing device for storage purposes only.
- c. Windows operating systems provide the functionality to allow users to create folders that are stored on their individual workstations that can be shared with others.⁵⁴

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

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

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

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

f. In addition, all employee workstations should be configured to use a software firewall. On August 25, 2004, Microsoft released its Windows Firewall as part of Windows XP Service Pack 2. This software firewall could be configured to block all incoming connection requests to a workstation. This would prevent, for example, users of

file-sharing applications, like LimeWire, from establishing a successful connection with a workstation and downloading shared files. The Windows Firewall accompanied the operating system at no cost to the customer.

g. Properly configuring firewalls at the network gateway and on employee workstations implements a defense in depth strategy for network protection. This provides protection at 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. Stealth⁵⁵ and OSSEC are examples of free products, and Tripwire is an example of a commercial product. These are the types of mechanisms that IT practitioners used regularly throughout the Relevant Time Period.

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

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

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

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

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

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

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

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

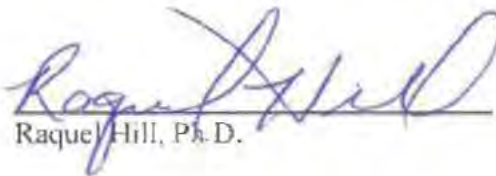
⁵⁷ See, for example, July 16, 2010 Letter from P. Ellis to A. Sheer (FTC-LABMD-002495 through FTC-LABMD-002503).

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

IX. Conclusion

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

Dated: March 18, 2014


Raquel Hill, Ph.D.

Appendix A

Home Address: School of Informatics and
734 E. Moss Creek Computing
Drive Indiana University
Bloomington, IN 47401 Bloomington, IN 47405
Phone(217)369-0105 Phone (812) 856-5807
hill raquel@gmail.com 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

Professional Experience

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

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

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

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

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

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

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

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

Grants

IBM Corporation, Equipment Grant – Cryptographic Co-processors

Equipment Value: \$75,000.00 Date: 9/01/05 – Present

CACR: Privacy Enhanced Online Human Subjects Data Collection

Total Award Amount: \$49,999.99 Date: 07/01/09 – 12/31/10

Role: PI Source of Support: IU

TC: Large: Collaborative Research: Anonymizing Textual Data and Its Impact on Utility

Total Award: \$568,895 Date: 9/01/10 – 8/31/14

Role: PI Source of Support: NSF

FRSP: Childhood Obesity Studies with Secure Cloud Computing

Total Award: \$36,500 Date: 9/1/11 – 12/31/13

Role: PI

Publications

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

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

Publications

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

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

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

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

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

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

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

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

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

Publications

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

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

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

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

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

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

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

Refereed Abstracts

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

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

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

- Refereed Abstracts** J. Al-Muhtadi, R. Hill, R. Campbell, A Privacy Preserving Overlay for Active Spaces, *Ubicomp Privacy Workshop in conjunction with the Sixth International Conference on Ubiquitous Computing*, Nottingham, England, September 2004.
- Posters**
- R. Hill, A.C. Solomon, E. Janssen, S. Sanders, J. Heiman, Privacy and Uniqueness in High Dimensional Social Science and Sex Research Datasets, Presented at the 37th Annual Meeting of the International Academy of Sex Research, August 10-13, 2011, Los Angeles, California.
- C. Boston, R. Hill, L. Moore, The Feasibility of Designing a Secure System to Prevent Surgical Errors Using RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.
- S. Camara, R. Hill, L. Moore, Understanding How RFID Technology Impacts Patient Privacy, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.
- R. Johnson, R. Hill, L. Moore, Evaluating and Mitigating the Security Vulnerabilities of RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.
- R. Hill, J. Wang, K. Nahrstedt, Quantifying Non-Functional Requirements: A Process Oriented Approach, *in the Proceedings of the 12th IEEE International Requirements Engineering Conference*, Kyoto, Japan, September 2004.
- Technical Reports** R. Hill, J. Al-Muhtadi, Building a Trusted Location Service for Pervasive Computing Environments, Technical Report, TR646, Computer Science, Indiana University, 2007.
- Dissertation** R. Hill, Sticky QoS: A Scalable Framework for Resource Reservations, Doctoral Dissertation in Computer Science, Harvard University Division of Engineering and Applied Sciences, November 2002.
- Symposiums** “Protecting Privacy in Sex Research: Challenges and solutions offered by new technologies and recommendations for the collection, protection and the sharing of multi-dimensional data”, **Speakers:** Raquel Hill, School of Informatics and Computing, Indiana University, Ulf-Dietrich Reips, iScience, University of Deusto, Bilbao, Spain, Stephanie Sanders, Gender Studies, Indiana University, The 38th Annual Meeting of the International Academy of Sex Research, July 8-12, 2012, Lisbon, Portugal
- Invited Talks** “Understanding the Risk of Re-Identification in Behavioral Science Data”, Technology in Government Topics in Privacy Seminar, Data Privacy Lab, Harvard University, Cambridge, MA, November 4, 2013.

Invited Talks

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

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

“Kinsey Goes Digital”, Kinsey Institute’s Board of Trustees Meeting, Indiana University, Bloomington, IN, May 20, 2011.

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

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

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

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

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

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

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

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

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

Invited Talks

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

“Overlay QoS”, Department of Computer Science, Auburn University, February 2004, Auburn, Alabama.

“Distributed Admissions Control for Sticky QoS”, *Ninth Annual Conference for African-American Researchers in the Mathematical Sciences*, June 2003, West LaFayette, Indiana.

“Distributed Admissions Control for Sticky QoS”. *Sixth Inform's Telecommunications Conference*, March, 2002, Boca Raton, Florida.

Former Congressman Lee Hamilton, Professor Fred Cate, and Professor Raquel Hill, “Security and Privacy in a Cyberwar World: A conversation about Edward Snowden, the NSA and the outlook for reform”, *Indiana Statewide IT Conference*, Indiana University, Bloomington, IN October, 29, 2013

Panels

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

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

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

Teaching

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

**Professional
Activities**

Member of Technical Program Committee

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

Member of Review Panel

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

Appendix B

Appendix B
Materials Considered or Relied Upon

IH Transcripts and Exhibits

13.02.05 Boyle, John - Transcript
13.02.05 Boyle, John - Exhibits
13.02.06 Daugherty, Michael - Transcript
13.02.06 Daugherty, Michael - Exhibit #8
13.02.06 Daugherty, Michael - Exhibit #14
13.02.06 Daugherty, Michael - Exhibit #23
13.05.02 Simmons, Alison - Transcript
13.05.02 Simmons, Alison - Exhibits
13.05.03 Kaloustian, Curt - Transcript
13.05.03 Kaloustian, Curt - Exhibits

Bates Range

FTC-000001-FTC-000115
FTC-000116-FTC-000376
FTC-000377-FTC-000416
FTC-000225-FTC-000246
FTC-000283-FTC-000304
FTC-000417-FTC-000423
FTC-000424-FTC-000493
FTC-000494-FTC-000512
FTC-000513-FTC-000638
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

10.02.24 Ellis Letter
10.06.04 Ellis Letter
10.07.16 Ellis Letter
10.07.16 Ellis Exhibits

Bates Range

FTC-LABMD-002506-FTC-LABMD-002520
FTC-LABMD-002523-FTC-LABMD-002524
FTC-LABMD-002495-FTC-LABMD-002503
FTC-LABMD-002505-FTC-LABMD-003131

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

Documents Produced by LabMD

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

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

Documents Produced by Tiversa

TIVERSA-FTC RESPONSE-000001-006904

Documents Produced by Sacramento Police Department

FTC-SAC-000001-FTC-LABMD-000044

Documents Produced by the Privacy Institute

FTC-PRI-000001-FTC-PRI-001719

Documents Produced by Cypress Communication, LLC

FTC-CYP-000001-FTC-CYP-000001
FTC-CYP-0001656-FTC-CYP-0001725
FTC-CYP-0001729-FTC-CYP-0001733
FTC-CYP-0001735-FTC-CYP-0001757

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

Documents Produced by ProviDyn, Inc.

FTC-PVD-000001-FTC-PVD-001582

Documents Produced by TrendMicro

FTC-TRM-000001-FTC-TRM-000455

Web Content Considered or Relied Upon

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

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

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

Articles & Publications

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

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

Books

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

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

FTC Provided Documents

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

Miscellaneous

- Federal Register, Department of Health and Human Services, “Standards for Privacy of Individually Identifiable Health Information” (October 15, 2002), <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrulet.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.