

ORIGINAL



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

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

**COMPLAINT COUNSEL’S OPPOSITION TO RESPONDENT’S
MOTION IN LIMINE TO LIMIT THE TESTIMONY OF ERIC JOHNSON**

The Court should deny Respondent’s Motion *in Limine* to Limit the Testimony of Eric Johnson because Respondent has failed to meet its high burden of establishing that the unspecified testimony it seeks to exclude is clearly inadmissible. Complaint Counsel seeks to introduce testimony from Dean Johnson about facts related to a study that he conducted on unauthorized disclosures of medical information, which Respondent contends is relevant to these proceedings. Dean Johnson has personal knowledge of those facts, and Respondent waived its argument to the contrary by not objecting to the testimony during its deposition of Dean Johnson.

BACKGROUND

On February 18, 2014, Respondent deposed M. Eric Johnson, Dean of Owen Graduate School of Management, Vanderbilt University, pursuant to a subpoena that it issued on February 12, 2014. Respondent questioned Dean Johnson at length about facts relating to a study that he conducted in 2008 entitled “Data Hemorrhages in the Health-Care Sector” (“Health-Care Data Hemorrhages Study”), including his research methodology and findings, and how the study was funded. *See* CX0721, Johnson Dep. Tr. with Compl. Counsel Designations (Attached as Exhibit

A); CX0382, Health-Care Data Hemorrhages Study (Attached as Exhibit B).¹ Following Respondent's examination, Complaint Counsel exercised its right as the non-noticing party to question Dean Johnson. Complaint Counsel also inquired about facts relating to Dean Johnson's Health-Care Data Hemorrhages Study, including his research methodology and findings, and the consequences of the inadvertent disclosure of consumers' personal information. *See* Ex. A (CX0721) at 92-125. At no time during Complaint Counsel's examination did Respondent object that Dean Johnson's testimony was based in speculation rather than fact, constituted improper expert opinion, or otherwise lacked foundation. *See id.*

On February 27, 2014, Complaint Counsel supplemented its Preliminary Witness List in light of additional information learned during discovery. Complaint Counsel's Supplemental Preliminary Witness List identified seven additional witnesses, including Dean Johnson. Complaint Counsel stated that Dean Johnson would "testify about facts related to [the Health-Care Data Hemorrhages Study], including his research methodology and findings . . . and the consequences of inadvertent disclosures of consumers' personal information." Resp. Mot., Ex. 1 (Compl. Counsel Suppl. Prelim. Witness List) at 3.

On March 14, 2014, Respondent sent a letter requesting that Complaint Counsel agree to "exclude any testimony [from Dean Johnson] about 'consequences of inadvertent disclosures of consumers' personal information'" ("March 14 Letter"). *See* Resp. Mot., Ex. 2. The March 14

¹ Dean Johnson conducted the Health-Care Data Hemorrhages Study, which was published in 2009, while he was a professor at Dartmouth College. *See* Ex. B (CX0382) at 1; Ex. A (CX0721) at 6, 9, 15. "Through an analysis of leaked files"—including the 1,718 page file identified in the Complaint as the "P2P insurance aging file"—the study examines "data hemorrhages stemming from inadvertent disclosures on internet-based file sharing networks." Ex. B (CX0382) at 1, 11-12; Compl. ¶ 17. The study also examines "the consequences of data hemorrhages, including privacy violations, medical fraud, financial identity theft, and medical identity theft." Ex. B (CX0382) at 1.

Letter also noted that Respondent was “willing to meet and confer regarding this matter” in the event that Complaint Counsel did not agree to limit Dean Johnson’s testimony as Respondent requested. *Id.*

On March 26, 2014, Complaint Counsel served its Final Proposed Witness List, which states that Dean Johnson will testify about the “facts related to [the Health-Care Data Hemorrhages Study]” identified in Complaint Counsel’s Supplemental Preliminary Witness List. Compl. Counsel Final Proposed Witness List (Mar. 26, 2014) at 16 (Attached as Exhibit C). The same day, Complaint Counsel served its designations from Dean Johnson’s deposition. *See* Ex. A (CX0721). On April 9, 2014, Respondent served its Final Proposed Witness List, which states that Respondent expects to call Dean Johnson as a live witness to testify on several topics, including “the facts underlying [the Health-Care Data Hemorrhages Study]” and communications related to his research methodology. Resp. Final Proposed Witness List (Apr. 9, 2014) at 3 (attached as Exhibit D). Respondent did not designate any testimony from Dean Johnson’s deposition.

On April 22, 2014, more than one month after sending the March 14 Letter, Respondent filed the present Motion. In the interim, Respondent did not request a time to meet and confer about its objection to Complaint Counsel’s introduction of Dean Johnson’s testimony. The parties nonetheless discussed the present Motion during their April 21, 2014 meet and confer session on other motions *in limine* and motions for *in camera* treatment, which the parties filed on April 22, 2014.

ARGUMENT**I. RESPONDENT HAS FAILED TO SHOW THAT THE UNSPECIFIED TESTIMONY IT SEEKS TO EXCLUDE IS CLEARLY INADMISSIBLE**

The party filing a motion *in limine* to exclude evidence faces a high burden. As this Court has explained, “[e]vidence should be excluded on a motion *in limine* only when the evidence is clearly inadmissible on all potential grounds.” *In re McWane, Inc.*, No. 9351, 2012 WL 3719035, at *3 (F.T.C. Aug. 16, 2012) (citing *Hawthorne Partners v. AT&T Techs., Inc.*, 831 F. Supp. 1398, 1400 (N.D. Ill. 1993)); *see also, e.g., In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 85, at *19 (Apr. 20, 2009) (same).

Respondent’s Motion should be denied because Respondent has failed to meet its high burden of establishing that the Court should exclude all testimony from Dean Johnson about “the consequences of inadvertent disclosures of consumers’ personal information.” Resp. Mot. at 4. Respondent fails to identify any specific testimony that it seeks to exclude, much less demonstrate that such unspecified testimony is “clearly inadmissible on all potential grounds.” *McWane*, 2012 WL 3719035, at *3. By not identifying particular testimony from Dean Johnson that it seeks to exclude, Respondent has failed to provide the Court with sufficient information to make an informed ruling on the admissibility of the testimony at issue. *See, e.g., Logan v. Cooper Tire & Rubber Co.*, No. 10–3–KSF, 2011 WL 3475273, at *2-3 (E.D. Ky. Aug. 9, 2011) (denying motion *in limine* because moving party “failed to identify any specific evidence that it [sought] to exclude” and court was therefore “unable to make an informed decision”); *Landers v. Nat’l R.R. Passenger Corp.*, No. Civ. 00-2233 (PAMJGL), 2002 WL 832588, at *3 (D. Minn. Apr. 26, 2002) (denying motion *in limine* because court was not provided “sufficient information to make an informed ruling on the admissibility of” the evidence at issue). Therefore, the Court should deny Respondent’s Motion and reserve judgment until trial, when the Court will have the

appropriate factual context—including Dean Johnson’s live testimony—to make an informed ruling on the testimony that Respondent seeks to exclude. *See In re POM Wonderful LLC*, No. 9344, 2011 WL 2160775, at *2 (May 5, 2011) (“Courts considering a motion *in limine* may reserve judgment until trial, so that the motion is placed in the appropriate factual context.”).

II. RESPONDENT SEEKS TO EXCLUDE ADMISSIBLE LAY TESTIMONY FROM DEAN JOHNSON AND HAS WAIVED ITS OBJECTIONS TO IT

Respondent’s Motion also should be denied because, contrary to Respondent’s assertion, Complaint Counsel seeks to introduce lay testimony from Dean Johnson that is based on fact, not speculation or expert opinion. As Complaint Counsel’s witness lists state, and as its deposition designations show, Complaint Counsel seeks to introduce testimony from Dean Johnson about facts related to his Health-Care Data Hemorrhages Study, including his research methodology and findings and the consequences of inadvertent disclosures of consumers’ personal information. *See* Resp. Mot., Ex. 1 (Compl. Counsel Suppl. Prelim. Witness List) at 3; Ex. C (Compl. Counsel Final Proposed Witness List) at 16; Ex. A (CX0721), at 92-125. Respondent has repeatedly contended that the facts surrounding Dean Johnson’s Health-Care Data Hemorrhages Study are relevant to these proceedings. *See, e.g.*, Sched. Conf. Tr. (Sept. 25, 2013) at 26-28; Resp. Opp’n to Compl. Counsel Mot. for Protective Order Re: Rule 3.33 Dep. (Feb. 26, 2014) at 3-5. Dean Johnson’s testimony about facts related to his Health-Care Data Hemorrhages Study is based on his personal knowledge from conducting the study, and Respondent waived its argument that any of Dean Johnson’s testimony lacked foundation by not objecting to it during his deposition. *See, e.g., In re WPMK, Inc.*, 42 B.R. 157, 159-60 (Bankr. D. Haw. 1984) (ruling that objections based on lack of foundation not made during deposition were deemed waived because they “might have been cured if presented at the deposition”); *see also* Fed. R. Civ. P. 32(d)(3)(A) (waiver of objections).

CONCLUSION

For the foregoing reasons, Respondent's Motion *in Limine* to Limit the Testimony of Eric Johnson should be denied. Respondent has failed to meet its high burden of establishing that the unspecified testimony from Dean Johnson that it seeks to exclude is clearly inadmissible.

Dated: April 29, 2014

Respectfully submitted,



Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown
Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-3713 – Lassack
Facsimile: (202) 326-3062
Electronic mail: mlassack@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on April 29, 2014, I filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

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

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

I further certify that I caused a copy of the foregoing document to be served through Secure File Transfer to:

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

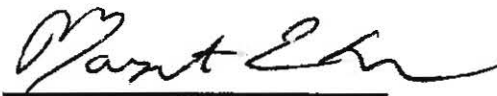
Reed Rubinstein
William A. Sherman, II
Sunni Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004

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

CERTIFICATE FOR ELECTRONIC FILING

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

April 29, 2014

By: 

Margaret Lassack
Federal Trade Commission
Bureau of Consumer Protection

Exhibit A

1
2 UNITED STATES OF AMERICA
3 BEFORE THE FEDERAL TRADE COMMISSION
4 OFFICE OF ADMINISTRATIVE LAW JUDGES
5 -----x

6 In the Matter of

7 DOCKET NO. 9357

8 LabMD, Inc.,
9 A corporation.

10 -----x
11 February 18, 2014
12 9:55 a.m.

13
14 Deposition of M. ERIC JOHNSON, Ph.D.,
15 taken by Respondent, pursuant to subpoena,
16 at the offices of Henry H. Korn, PLLC, 220
17 East 42nd Street, New York, New York 10017,
18 before Alexis Perez Jenio, a Shorthand
19 Reporter and Notary Public of the State of
20 New York.

1
2 APPEARANCES (Continued):

3
4
5 DARTMOUTH COLLEGE,
6 OFFICE OF THE GENERAL COUNSEL
7 63 South Main Street, suite 301
8 Hanover, New Hampshire 03755
9 BY: KEVIN D. O'LEARY

10
11
12 PRESENT: MICHAEL J. DAUGHERTY, LabMD
13
14
15
16
17
18
19
20
21
22
23
24
25

1
2 APPEARANCES:

3
4
5 DINSMORE & SHOHL, LLP
6 Attorneys for respondent
7 801 Pennsylvania Avenue, N.W.,
8 Suite 610
9 Washington, DC 20004

10 BY: WILLIAM A. SHERMAN, II

11
12
13 FEDERAL TRADE COMMISSION
14 BUREAU OF CONSUMER PROTECTION
15 600 Pennsylvania Avenue, N.W.
16 Mail Stop NJ-3158
17 Washington, DC 20580

18 BY: LAURA RIPOSO VAN DRUFF
19 ALAIN SHEER
20
21
22
23
24
25

1 Johnson
2 M. ERIC JOHNSON, Ph.D.,
3 called as a witness, having been duly
4 sworn, testified as follows:

5 EXAMINATION
6 BY MR. SHERMAN:
7 Q. Good morning, Dr. Johnson. My
8 name is William Sherman. I represent
9 LabMD, and you're here by subpoena. Is
10 that correct?

11 A. Yes.

12 Q. I'm going to show you what will
13 be marked as Exhibit 1.

14 MR. SHERMAN: We're going to do
15 RX and a number.

16 MR. SHEER: You guys have been
17 using RX-1 previously, so at some point
18 down the road you might think about
19 starting at a higher number.

20 MR. SHERMAN: Will you mark this
21 RX-1, please?

22 (One-page cover letter with
23 attached Subpoena ad Testificandum
24 marked Exhibit RX-1 for identification)

25 Q. I'm showing you what has been

5

1 Johnson
 2 **marked RX-1. If you could take a look at**
 3 **that for me and just confirm that you have**
 4 **seen it, or your lawyer has advised you,**
 5 **and that it was sent to him and that you're**
 6 **here by virtue of this subpoena.**
 7 MS. RIPOSO VAN DRUFF: Counsel,
 8 do you have a copy for me?
 9 MR. SHERMAN: I do. I suspect
 10 that you've seen it, but you can have
 11 my copy.
 12 MS. RIPOSO VAN DRUFF: Thank you.
 13 A. I think there may be some other
 14 things that are attached to this that I
 15 haven't seen before.
 16 MR. O'LEARY: The last page --
 17 well, our last page, anyway, I think
 18 this was just a copy.
 19 MR. SHERMAN: Yes. That's not
 20 even intended to be attached. I don't
 21 how that got attached.
 22 **Q. Other than that last page --**
 23 A. Yes.
 24 **Q. -- which was inadvertently**
 25 **attached, you would agree that you've seen**

6

1 Johnson
 2 **the document marked as RX-1?**
 3 A. Yes.
 4 **Q. If you could, just give me your**
 5 **educational background, starting with your**
 6 **college education.**
 7 A. Yes. So I have Bachelor of
 8 Science in economics from Penn State, a
 9 Bachelor of Industrial Engineering from
 10 Penn State, a Master's of Industrial
 11 Engineering from Penn State, and a Ph.D. in
 12 industrial engineering from Stanford.
 13 **Q. Could you give me, let's say, the**
 14 **past ten years of your employment history?**
 15 A. Past ten years would include time
 16 as a professor at Dartmouth College in the
 17 Tuck School of Business in various roles
 18 there, including director of the Center for
 19 Digital Strategies.
 20 **Q. Was that "digital strategies"?**
 21 A. Um-hmm. Yes.
 22 **Q. Let me back up. And it's**
 23 **Dr. Johnson --**
 24 A. Yes.
 25 **Q. -- is that what you prefer?**

7

1 Johnson
 2 A. Yes.
 3 **Q. Have you ever had your deposition**
 4 **taken before?**
 5 A. No.
 6 **Q. So let me go over a few kind of**
 7 **ground rules.**
 8 **The court reporter is here.**
 9 **She's taking down everything that we say,**
 10 **and so it's important that you respond**
 11 **verbally with a "yes" or a "no" rather than**
 12 **an "um-hmm" or an "uh-huh," because those**
 13 **can be misconstrued or misunderstood.**
 14 **Secondly, I'll be asking the**
 15 **questions. And if you could wait until I**
 16 **finish asking the question before you**
 17 **answer, and I'll wait until you answer**
 18 **before asking you another, that will help**
 19 **the court reporter also take down**
 20 **everything we say. It doesn't translate**
 21 **well when we talk over one another.**
 22 **If at any time you wish to take a**
 23 **break, feel free to say, Hey, I need to**
 24 **take a break, and we'll do so. I'll just**
 25 **ask that if there's a question on the**

8

1 Johnson
 2 **table, that you respond to that question**
 3 **before taking a break.**
 4 **At any time you are free to**
 5 **consult with your counsel. And although**
 6 **this is basically an informal setting, it**
 7 **is just as important as if you were in**
 8 **front of a court of law before a judge and**
 9 **a jury, that you tell the truth. You**
 10 **understand that, right?**
 11 A. Yes.
 12 **Q. Those are usually the only ground**
 13 **rules that I have. And if you try to**
 14 **follow those, then I think it will do well**
 15 **for the court reporter, make for a nice,**
 16 **clean transcript, and we'll move along**
 17 **pretty quickly. Agreed?**
 18 A. Yes.
 19 **Q. Okay. Thank you.**
 20 **So it seems that ten years wasn't**
 21 **quite far back enough, because the past ten**
 22 **years you've been basically affiliated with**
 23 **Dartmouth College. Is that correct?**
 24 A. Until six months ago, when I
 25 **joined Vanderbilt University. Or more than**

1 Johnson
 2 since months ago. In fact, it would be
 3 July 1st.
 4 Q. So July 1st of 2013 you joined
 5 Vanderbilt. Is that correct?
 6 A. Yes.
 7 Q. In what capacity?
 8 A. As dean of the business school.
 9 Q. Prior to Dartmouth College, how
 10 were you employed?
 11 A. As a professor at Vanderbilt
 12 University.
 13 Q. In what area?
 14 A. The School of Management.
 15 Q. Is it fair to say that your
 16 employment history has basically been in
 17 academia, or have you worked in industry?
 18 A. Prior to that, I worked at
 19 Hewlett-Packard.
 20 Q. In what capacity?
 21 A. As a development engineer.
 22 Q. Developing what?
 23 A. We were -- I was part of a
 24 laboratory that was working on
 25 computer-driven manufacturing.

1 Johnson
 2 glance that I'm making right now leads me
 3 to believe that I have not seen this
 4 before.
 5 Q. What I believe that document is
 6 is a series of contracts and amendments
 7 between Dartmouth College Board of Trustees
 8 and the Department of Homeland Security.
 9 And if you look on the first page of that
 10 document, it states, "Agreement No.
 11 2006-CS-001-000001." Do you see that?
 12 A. Yes.
 13 Q. And the title is "Cyber Security
 14 Collaboration and Information Sharing." Do
 15 you see that?
 16 A. Yes.
 17 Q. Would you describe part of your
 18 work at Dartmouth as being associated or
 19 related to cyber security collaboration and
 20 information sharing?
 21 A. Yes.
 22 Q. But you've not seen these
 23 documents. Is that correct?
 24 A. I don't believe so. Not in this
 25 form, anyways.

1 Johnson
 2 Q. So it's my understanding that
 3 Dartmouth College had a contract with the
 4 Department of Homeland Security to do
 5 certain research. Is that an accurate
 6 statement?
 7 A. Yes.
 8 Q. And as a result of that contract,
 9 is it fair to say that the article "Data
 10 Hemorrhages in The Health Care Sector" was
 11 written and published by you?
 12 A. Yes.
 13 Q. I'm going to show you what I'd
 14 like to have the court reporter mark as
 15 RX-2.
 16 (Homeland Security Grant Award
 17 Terms and Conditions marked Exhibit
 18 RX-2 for identification)
 19 Q. Have you taken a look at RX-2,
 20 please?
 21 A. I don't believe I've seen this
 22 document before.
 23 Q. You've not seen any part of that
 24 document?
 25 A. There are many pages here, but a

1 Johnson
 2 Q. Now, did you have any contact
 3 with the Department of Homeland Security
 4 with regard to your research?
 5 A. Define "contact."
 6 Q. Telephone calls, e-mails,
 7 meetings, negotiations, discussions of
 8 terms of contracts.
 9 A. This work was initiated by a
 10 proposal to the Department of Homeland
 11 Security --
 12 Q. Who made the proposal?
 13 A. -- which I participated in, along
 14 with many others.
 15 Q. So you did participate in the
 16 proposal for what you believe this contract
 17 is associated with?
 18 A. Yes.
 19 Q. And when was the proposal made?
 20 A. Prior to initiating the work.
 21 But I would have to go back and look at my
 22 calendar to look at the exact dates.
 23 Q. When did the work initiate?
 24 A. This was a multi-year grant, and
 25 work was conducted over a number of years,

1 Johnson
 2 including 2008. But prior to 2008, 2007,
 3 and 2009, so in that time period. I would
 4 have to look at my calendar to know the
 5 exact dates.
 6 **Q. And I'm not asking you for exact**
 7 **dates.**
 8 **But is it fair to then**
 9 **characterize your testimony as the work**
 10 **associated with these contracts initiated**
 11 **in 2007?**
 12 A. There may have been grant
 13 proposal efforts before that time.
 14 **Q. Well, I'm just interested in when**
 15 **the work initiated.**
 16 A. So I guess you'll have to define
 17 "work."
 18 **Q. Well --**
 19 MR. O'LEARY: Could I just ask a
 20 question --
 21 MR. SHERMAN: Sure.
 22 MR. O'LEARY: -- that may be
 23 helpful?
 24 MR. SHERMAN: Sure.
 25 MR. O'LEARY: Are you asking

1 Johnson
 2 **article "Data Hemorrhages in the Healthcare**
 3 **Sector." You're familiar with that**
 4 **article. Is that correct?**
 5 A. Yes.
 6 **Q. You're the author of that**
 7 **article. Is that correct?**
 8 A. Yes.
 9 **Q. When was it published?**
 10 A. It was published in 2009.
 11 **Q. And are you aware of when the**
 12 **grant was awarded that, I guess, funded the**
 13 **research for this article?**
 14 A. One clarification there is that
 15 this work wasn't solely funded by that
 16 grant.
 17 **Q. Okay.**
 18 A. It was partially funded by that
 19 grant. And the time period at which that
 20 work was done is clearly outlined in the
 21 article itself.
 22 **Q. Well, when do you recall the work**
 23 **being done?**
 24 A. It was primarily done in 2008.
 25 MR. SHERMAN: Why don't we mark

1 Johnson
 2 about the work on the proposal or the
 3 research that the grant funded?
 4 MR. SHERMAN: I'm asking him for
 5 the work on the research that the grant
 6 funded.
 7 **Q. And I was using "work initiated"**
 8 **because it was a term that you used that I**
 9 **thought you might be comfortable with.**
 10 A. Yeah.
 11 **Q. And I thought you might have had**
 12 **a definition for it yourself, because you**
 13 **used it. But if not, we're talking about**
 14 **the work that initiated after the grant of**
 15 **the proposal.**
 16 A. And the reason that I'm being
 17 specific is that there were more than one
 18 grant from the Department of Homeland
 19 Security over a number of years that were
 20 related to cyber security, and you're
 21 asking about one very specific one, so I
 22 just want to be sure that we're clear.
 23 **Q. Okay. Then let's try to be more**
 24 **clear.**
 25 **I'm interested in the**

1 Johnson
 2 the article as RX-3, then.
 3 (Article titled "Data Hemorrhage
 4 on the Healthcare Sector," Bates
 5 stamped Eric Johnson - 000003 through
 6 24, marked Exhibit RX-3 for
 7 identification)
 8 **Q. So the article that we're**
 9 **referring to is the article that's now been**
 10 **marked as RX-3. Would you agree?**
 11 A. I agree.
 12 **Q. And you indicated in our**
 13 **discussion about RX-2 that the article was**
 14 **partially funded by the Department of**
 15 **Homeland Security?**
 16 A. That's correct.
 17 **Q. Were there any other funding**
 18 **sources for the work and the research that**
 19 **went into the article?**
 20 A. As part of a professor's job at
 21 university, research is often funded as
 22 part of their salary.
 23 **Q. Any other sources of funding?**
 24 A. No, not that I'm aware of.
 25 **Q. What is the Institute of**

17

1 Johnson
 2 **Information Infrastructure Protection?**
 3 A. It's a consortium of universities
 4 and laboratories that work together to
 5 conduct research on information security.
 6 **Q. Did the consortium participate in**
 7 **the "Data Hemorrhaging" article?**
 8 A. How do you define "participate"?
 9 **Q. Well, you said the consortium**
 10 **worked together. Did they work together in**
 11 **any respect, whether it be sharing research**
 12 **or ideas, on the "Data Hemorrhaging"**
 13 **article?**
 14 A. The proposal that we referred to
 15 earlier, RX-2, was funded as part of a
 16 consortium effort, and, as you will see
 17 from that document, there were many pieces
 18 to the project conducted by many different
 19 researchers at different institutions. The
 20 work conducted on the "Data Hemorrhaging"
 21 article was conducted at Dartmouth College
 22 by myself.
 23 **Q. So was any portion of the funding**
 24 **for the consortium used for the "Data**
 25 **Hemorrhaging" article, other than, I think**

18

1 Johnson
 2 **you indicated in your testimony, that this**
 3 **funding for the proposal came through the**
 4 **I3P. That's what it's called, isn't it?**
 5 MS. RIPOSO VAN DRUFF: Objection;
 6 misstates testimony.
 7 A. The proposal was prepared by
 8 members of the I3P and submitted to the
 9 Department of Homeland Security by those
 10 members.
 11 **Q. And was the "Data Hemorrhaging"**
 12 **article part of that proposal?**
 13 A. Yes.
 14 **Q. And was --**
 15 A. Though, of course, it was a
 16 proposal at that time, so a proposal is not
 17 specific in terms of the exact form of the
 18 research.
 19 **Q. So would it be fair to say that**
 20 **the "Data Hemorrhaging" article came about**
 21 **as a result of the proposal?**
 22 A. Yes.
 23 **Q. And so there was funding granted**
 24 **for that proposal?**
 25 A. Yes.

19

1 Johnson
 2 **Q. And it came through the**
 3 **Department of Homeland Security. Is that**
 4 **correct?**
 5 A. Yes.
 6 **Q. So during the proposal process, I**
 7 **think you've indicated that you**
 8 **participated, and that you -- well, let me**
 9 **put it this the way: Did you have meetings**
 10 **with the Department of Homeland Security**
 11 **during the proposal process that you**
 12 **attended?**
 13 A. The proposal itself was a written
 14 proposal that was submitted to the
 15 Department of Homeland Security as part of
 16 a call for proposals. It would
 17 customarily, and I think in this case, go
 18 through a peer-review process.
 19 Reviews from that peer-review
 20 process would then be provided to the
 21 research team, and the research team is
 22 often given the opportunity to respond to
 23 those reviews.
 24 **Q. Are those reviews conducted by**
 25 **the Department of Homeland Security?**

20

1 Johnson
 2 A. They're conducted by a peer
 3 review group, typically not members of the
 4 Department of Homeland Security. Though
 5 the membership of that peer review is not
 6 provided to the grant proposal writers. It
 7 is what's called a "blind process."
 8 **Q. So is it your understanding,**
 9 **then, that upon submission of your**
 10 **proposal, that the Department of Homeland**
 11 **Security submits it to a peer review group**
 12 **of their choosing for evaluation?**
 13 A. Yes.
 14 **Q. In terms of the "Data**
 15 **Hemorrhaging" article, were there any other**
 16 **persons from Dartmouth who worked on the**
 17 **article with you?**
 18 A. Some graduate students. I think
 19 some of them are mentioned in the
 20 acknowledgments in the paper.
 21 **Q. That's the extent?**
 22 A. Yeah. Also, it's noted.
 23 I think you asked specifically
 24 from Dartmouth?
 25 **Q. I did.**

1 Johnson
 2 A. Okay.
 3 **Q. And how many graduate students**
 4 **from Dartmouth?**
 5 A. I think in this particular case,
 6 one in particular, though there may have
 7 been others who participated in some way in
 8 a less meaningful or substantial way.
 9 **Q. The one in particular, can you**
 10 **give me that person's name?**
 11 A. Nicholas Willey.
 12 **Q. I see him in the acknowledgments.**
 13 **Is that correct?**
 14 A. That's correct.
 15 **Q. And what was Mr. Willey's role?**
 16 **What did he actually do?**
 17 A. Mr. Willey would conduct
 18 background research on areas related to the
 19 paper, perform various data analysis
 20 functions, creating graphics, looking for
 21 references.
 22 **Q. I notice within the article there**
 23 **are references to recorded complaints as**
 24 **noted by the FTC. Is that the type of**
 25 **background research Mr. Willey would have**

1 Johnson
 2 **done?**
 3 A. Looking for published related
 4 articles, yes.
 5 **Q. And do you know if Mr. Willey**
 6 **conducted that research with regard to FTC**
 7 **and the recorded complaints that they had?**
 8 A. What do you mean by "conducted"?
 9 **Q. Well, did he come up with the**
 10 **information, or was it provided from some**
 11 **other source?**
 12 A. I think it was referenced there
 13 as a secondary resource source, what we
 14 would call "literature review."
 15 **Q. Okay.**
 16 A. I would also say that that work
 17 could have very well been work that I did.
 18 **Q. Okay. So this information wasn't**
 19 **provided to you by the FTC?**
 20 A. That's correct.
 21 **Q. Dr. Johnson, I noticed in RX-2,**
 22 **as I was skimming through it, that there is**
 23 **no mention of Tiversa at all. How did**
 24 **Tiversa become involved in the "Data**
 25 **Hemorrhaging" article?**

1 Johnson
 2 A. Oh, RX-2. I'm sorry.
 3 Tiversa has been a research
 4 partner of mine for a number of years.
 5 **Q. How long?**
 6 A. Prior to that work, at least two
 7 or three years, maybe longer.
 8 **Q. So it's fair to say that Tiversa**
 9 **has been a research partner of yours since**
 10 **around 2005?**
 11 A. I couldn't be sure if that was
 12 the initiation. It could have been
 13 earlier.
 14 **Q. And how did you initially come in**
 15 **contact with Tiversa?**
 16 A. I became interested in studying
 17 different forms of information breaches,
 18 and in particular, breaches that we would
 19 call inadvertent breaches, and I became
 20 aware of Tiversa because of my interests in
 21 that work.
 22 **Q. I'm still kind of -- you've told**
 23 **me generally how. I want to know more**
 24 **specifically.**
 25 **Did you make a phone call to**

1 Johnson
 2 **Tiversa? Did you bump into someone on the**
 3 **street that just so happened to be from**
 4 **Tiversa?**
 5 A. I think I was introduced to them
 6 by a mutual friend.
 7 **Q. Do you recall who from Tiversa**
 8 **you were introduced to?**
 9 A. I believe it was Chris -- and I
 10 think the last name is Gomery (sic). I
 11 wonder if he's mentioned here. No, I don't
 12 think so.
 13 **Q. Gormley?**
 14 A. Gormley.
 15 **Q. Does that ring a bell?**
 16 A. There you go.
 17 It's great when you know my
 18 friends.
 19 **Q. That was a softball. I'm going**
 20 **to let it go.**
 21 **Have you done any other research**
 22 **other than the "Data Hemorrhaging" article**
 23 **that you've used Tiversa's technology for?**
 24 A. Yes.
 25 **Q. What other research would that**

1 Johnson
 2 **be?**
 3 A. We conducted a project examining
 4 leaks or inadvertent disclosures from
 5 financial institutions. We also conducted
 6 research examining criminal elements within
 7 peer-to-peer file sharing networks. You
 8 can find in my vitae several papers related
 9 to that and related work.
 10 **Q. Any other research with Tiversa?**
 11 A. Work after this, examined
 12 subsequent leaks from the health care
 13 sector post high tech, which was the
 14 Federal incentive program that initiated
 15 payments to hospitals to install
 16 information technology.
 17 **Q. Is that the extent of it?**
 18 A. So I think in total there's a
 19 series of several different projects
 20 spanning banking and health care and
 21 identity theft.
 22 **Q. And do all of these projects**
 23 **utilize Tiversa's technology to gather**
 24 **information concerning identity theft data**
 25 **breaches, data leaks, things of that**

1 Johnson
 2 **nature?**
 3 A. Yeah, specifically file transfers
 4 on peer-to-peer file sharing networks, and
 5 also search patterns of peer-to-peer file
 6 sharing users.
 7 **Q. You've named four projects: leaks**
 8 **from financial institutions; criminal**
 9 **elements within peer-to-peer networks; the**
 10 **"Data Hemorrhaging" article, which is RX-3;**
 11 **and then a project also concerning leaks**
 12 **from the health care sector post high-tech.**
 13 A. Yes.
 14 **Q. For each of those projects, was**
 15 **the technology that you used from Tiversa**
 16 **focused in on file sharing and/or specific**
 17 **users of peer-to-peer networks?**
 18 MS. RIPOSO VAN DRUFF: Objection;
 19 compound.
 20 A. That research was all using
 21 technology that examined file movement and
 22 availability on peer-to-peer file sharing
 23 networks -- and when we say "networks," the
 24 plural is intentional -- and also user
 25 searches in those networks.

1 Johnson
 2 **Q. And so you did user searches in**
 3 **all four of the projects that I just named?**
 4 MS. RIPOSO VAN DRUFF: Objection;
 5 vague as to "user searches."
 6 A. In both the financial sector and
 7 health care sector projects, we gathered
 8 information on user searches. But there
 9 were other elements of research where we
 10 were not looking at user searches.
 11 **Q. For example, that would be the**
 12 **file sharing aspect of the research. Is**
 13 **that correct?**
 14 A. Yes. And subsequently, the
 15 analysis of files we found in file sharing
 16 networks.
 17 **Q. Let's look at RX-3, then, and**
 18 **maybe that will give us some more insight**
 19 **into how this actually works.**
 20 If you'll notice, at the top
 21 right hand of every page there's your name
 22 and then there's a series of numbers. I
 23 will refer to the page based on that number
 24 at the top right hand. Is that agreeable?
 25 A. Yup.

1 Johnson
 2 **Q. So on page 3, which actually is**
 3 **the first page, you indicate in**
 4 **Footnote 1 -- and I'm going to read it, and**
 5 **correct me if I misstate something --**
 6 **"Experiments described in this paper were**
 7 **conducted in collaboration with Tiversa who**
 8 **has developed a patent-pending technology**
 9 **that, in real-time, monitors global P2P**
 10 **file sharing networks." Did I read that**
 11 **correctly?**
 12 A. I believe so.
 13 **Q. Do you have an understanding of**
 14 **what that really means and what it is that**
 15 **Tiversa is able to do in terms of**
 16 **monitoring file sharing networks?**
 17 A. Yes.
 18 **Q. How does Tiversa monitor a file**
 19 **sharing network?**
 20 A. They participate in that network
 21 as a node in the network.
 22 **Q. That's a different function than**
 23 **using the network as a user. Would you**
 24 **agree?**
 25 A. It could look similar.

1 Johnson
 2 **Q. "It could look similar" is your**
 3 **response, but is it different than what a**
 4 **user would be doing on the network?**
 5 A. Different in what way?
 6 **Q. Well, that is the question.**
 7 **You indicated that you understood**
 8 **what that technology did, and my question,**
 9 **at its core, is: How does the technology**
 10 **allow Tiversa to function differently than**
 11 **a user of the network?**
 12 MS. RIPOSO VAN DRUFF: Objection;
 13 foundation.
 14 A. I think to an outside observer,
 15 that would be viewed as a user.
 16 **Q. Okay. Well, what about to you,**
 17 **how do they appear, based on your knowledge**
 18 **of the technology and how it works?**
 19 MS. RIPOSO VAN DRUFF: Objection;
 20 vague as to "appear."
 21 A. A typical user would participate
 22 in the network through a single computer;
 23 Tiversa would use multiple computers, thus,
 24 looking like multiple users.
 25 **Q. Is that the only difference?**

1 Johnson
 2 **You described it as they**
 3 **participate in the network as a node?**
 4 A. Or nodes.
 5 **Q. Or nodes.**
 6 A. That's, "users" and "nodes" are
 7 equivalent in my nomenclature.
 8 **Q. Are there any other differences**
 9 **that you can articulate between how**
 10 **Tiversa's technology allows them to**
 11 **participate in the network, or on the**
 12 **network, that's not typical of a typical**
 13 **user?**
 14 MS. RIPOSO VAN DRUFF: Objection;
 15 vague as to "typical."
 16 A. I'm not sure I understand what
 17 you're asking.
 18 **Q. Well, I'm asking -- to your**
 19 **understanding of Tiversa's technology, I'm**
 20 **asking the same question: How does it**
 21 **allow them to participate on the network**
 22 **which is different than a user?**
 23 MS. RIPOSO VAN DRUFF: Objection;
 24 lacks foundation.
 25 A. Other users could participate in

1 Johnson
 2 a similar way.
 3 **Q. So is it fair to characterize**
 4 **your testimony that, according to your**
 5 **understanding of Tiversa's technology, the**
 6 **main difference that you can articulate is**
 7 **that Tiversa is able to participate on the**
 8 **network as a node multiple times?**
 9 MS. RIPOSO VAN DRUFF: Objection.
 10 **Q. Because they have multiple**
 11 **computers.**
 12 MS. RIPOSO VAN DRUFF: Misstates
 13 prior testimony.
 14 A. They would use multiple
 15 computers. The structure of these
 16 peer-to-peer file sharing networks are such
 17 that having multiple nodes is a distinct
 18 advantage in terms of being able to capture
 19 the activity of users on the network.
 20 **Q. What do you mean by "capture the**
 21 **activity"?**
 22 A. Typically, these networks allow
 23 users to share files and search for files.
 24 But when a user places a search in a
 25 network, for example, using a LimeWire

1 Johnson
 2 client, they may only successfully see
 3 other holders of that file within a few
 4 nodes of them; that is to say, when they
 5 issue a search, that search is not
 6 exhaustive of the entire network of users
 7 who are operating at that moment using the
 8 Gnutella network, LimeWire being a client
 9 on the Gnutella network.
 10 By having multiple nodes, they're
 11 able to see multiple subnetworks, parts of
 12 the network, and perform a more exhaustive
 13 search than a single user.
 14 **Q. Would a single user be searching**
 15 **for a file, whether that file be digital**
 16 **video or data or a report, but Tiversa**
 17 **would be looking at what that user was**
 18 **looking for?**
 19 I'm just not understanding -- it
 20 appears to me, and please correct me if I'm
 21 wrong, that a user of the network is
 22 searching for something. Is that correct?
 23 A. That's correct.
 24 **Q. But that Tiversa is searching for**
 25 **what, the user?**

1 Johnson
2 A. These networks are a little
3 different than maybe the network you're
4 envisioning. When a user issues a search,
5 say that user wants a song from Madonna and
6 they issue a search for "Material Girl,"
7 that string, "Material Girl," is passed to
8 other users of that network to see if they
9 have a match.

10 If a user doesn't have a match,
11 the string gets passed to another user and
12 then to another user. But there's no
13 guarantee when a user issues that search
14 that that string, "Material Girl," will get
15 passed to every computer on the network.
16 In fact, typically, depending on the
17 network -- and there are many, many
18 exceptions to what I'm saying here, because
19 there are many different networks, all of
20 them developed primarily by open-sourced
21 communities.

22 But typically, that search would
23 be passed to a limited number of computers,
24 and some of those computers are users, may
25 be considered super nodes or über nodes.

1 Johnson
2 which have information that might speed the
3 search, sending it to a more likely user.
4 But the key feature of these networks is
5 that there's no one super user that knows
6 all the network, a key distinction from the
7 failed Napster.

8 Napster was driven out of
9 business because they were maintaining a
10 list of every file by every user, allowing
11 you to quickly find the file. This one
12 looks more like a whispering game: I ask
13 you; you ask Michael; Michael asks Kevin;
14 and we keep a little trail, so that if
15 Kevin does have the file, he knows kind of
16 how to get back to the original requester.

17 That is a layman's description of
18 how these networks work. There are many
19 technical subtleties, enhancements. The
20 networks are constantly changing, growing,
21 contracting.

22 Q. You used the term "string." Is
23 that synonymous with the layman's term for
24 "search"?

25 A. A set of text related to a

1 Johnson
2 search.

3 Q. So let's turn to page 4 of RX-3.
4 In the first full paragraph on that page,
5 about, I don't know, one-third of the way
6 down that paragraph, there's a sentence.
7 You say, "These files were inadvertently
8 published in popular peer-to-peer file
9 sharing networks like LimeWire or BearShare
10 and could be easily downloaded by anyone
11 searching for them." Do you see that
12 sentence?

13 A. Yes.

14 Q. Did I read it correctly?

15 A. Yes.

16 Q. Your statement is that they could
17 be easily downloaded?

18 A. Yes.

19 Q. "Downloading" is what?

20 A. Is sharing the file.

21 Q. So they could take the
22 information from the network, or from that
23 individual working on the network who had
24 the file that they were looking for, and
25 download it onto their computer. Is that

1 Johnson
2 an accurate statement?

3 A. Yes, but only if the user was
4 sharing that file.

5 Q. I see.

6 A. That is, making it publicly
7 available on the network.

8 Q. There's also another piece, isn't
9 there, which includes not only the users
10 sharing the file on the network, but the
11 other party has to be looking for the file.
12 Is that correct?

13 A. That is correct. Or, more
14 precisely, looking for something that
15 somehow matches with that file. So a user
16 searching for "lab," might only find songs
17 with the name "lab." They might find
18 spreadsheets with "lab" in the title or in
19 the metadata of that file. They need not
20 be searching for a specific file.

21 Q. But they need to be searching for
22 something that is related to a file which
23 another user on the network is sharing?

24 A. Yes.

25 Q. In terms of using Tiversa's

1 Johnson
 2 technology for the "Data Hemorrhaging"
 3 article, how did you get the information?
 4 For example, you indicated that, in your
 5 article, that during the first phase of
 6 your study, that there were 3,328 files
 7 collected by random sampling. How did you
 8 collect the files?
 9 A. I believe the paper explicitly
 10 details exactly how we collected the files.
 11 Q. Well, it uses the
 12 words "collected the files," and it does
 13 give a frame work. I guess what I'm
 14 looking for is, were the files transferred
 15 from Tiversa to a computer at Dartmouth, or
 16 were the files printed off from Tiversa and
 17 mailed to Dartmouth, or was Dartmouth given
 18 remote access to Tiversa's system and
 19 collection activities?
 20 A. We used different methods to
 21 share information. Because of the size and
 22 extent of the findings and the file
 23 transfer technology at that time, in some
 24 cases the files were shipped to us on DVD
 25 or hard drive; in some cases we were

1 Johnson
 2 provided access through an FTP server that
 3 will allow us to review the files remotely.
 4 Q. Were these the only two methods
 5 used?
 6 A. No, I think there may have been
 7 others. Possibly, in some cases by e-mail,
 8 though typically, only in cases of maybe a
 9 single file.
 10 Q. You describe in your paper, on
 11 the very first page, you say that the
 12 research focused on inadvertent
 13 disclosures. Do you agree with that?
 14 A. Yes.
 15 Q. How do you know that the
 16 disclosures were inadvertent?
 17 A. Presumed inadvertent on our part.
 18 Q. Because?
 19 A. Because these networks were
 20 primarily used by individuals sharing
 21 music, video, and pictures. But it's
 22 possible that users may wish to share some
 23 of these files and had planned to do so, so
 24 it's a presumption on our part.
 25 Q. Do you think it was a safe

1 Johnson
 2 presumption?
 3 A. In many cases, not all.
 4 Q. And why do you think it was a
 5 safe presumption at the time you were doing
 6 the research?
 7 A. Well, first of all, some of the
 8 files that were being shared would have
 9 been harmful to the individuals, create
 10 potential risks for those individuals.
 11 Q. Based on your work in this area
 12 with regard to peer-to-peer file sharing
 13 networks, when you were doing the research
 14 back in 2008, 2009 – is that fair to
 15 say? – what was the level of awareness in
 16 terms of users with regard to some of the
 17 dangers of using peer-to-peer networks?
 18 MS. RIPOSO VAN DRUFF: Objection;
 19 vague and as to state of mind of the
 20 users.
 21 A. Much of our research,
 22 particularly our first papers in each area,
 23 were really there to create more awareness
 24 for the risks that we believed many users
 25 weren't aware of.

1 Johnson
 2 Q. And in 2008, would it be fair to
 3 say that it was your position that, still,
 4 many users were not aware of the file
 5 sharing capabilities of these peer-to-peer
 6 networks?
 7 MS. RIPOSO VAN DRUFF: Objection;
 8 vague as to "users."
 9 A. Yes.
 10 Q. Page 10 of your article sets out
 11 the research method and analysis. And you
 12 indicate that -- and this is the second
 13 sentence under Section 4, "Research Method
 14 and Analysis" -- "To collect a sample of
 15 leaked data, we initially focused on
 16 Fortune Magazine's list of the top ten
 17 publicly traded health-care firms."
 18 Why did you focus in on the top
 19 ten?
 20 A. We were following research
 21 protocol from our work in banking, where we
 22 believed that focusing on the largest
 23 providers would give us a broad section, a
 24 cross section, of the leak activity in the
 25 health care sector.

1 Johnson
 2 **Q. Was there also a consideration**
 3 **given to focusing in on the top ten, that**
 4 **there would be a more sophisticated system**
 5 **in place to protect the data?**
 6 A. Possibly, but I don't think that
 7 was a specific objective we had in mind.
 8 MS. RIPOSO VAN DRUFF: William,
 9 would this be a good time to take a
 10 break?
 11 MR. SHERMAN: Sure.
 12 (Four-page e-mail string marked
 13 Exhibit RX-4 for identification)
 14 EXAMINATION CONTINUED
 15 BY MR. SHERMAN:
 16 **Q. Keep that open, but we've marked**
 17 **a document, RX-4.**
 18 **We were talking about the top ten**
 19 **hospitals before we took a short break.**
 20 **And if you could turn to the first page --**
 21 **actually, it's the last page, but it's**
 22 **marked "1 of 4."**
 23 **What this appears to be is an**
 24 **e-mail from you sent to Chris Gormley, and**
 25 **it appears to be a list of top ten**

1 Johnson
 2 **hospitals or health care facilities.**
 3 A. Yup.
 4 **Q. Is that what that represents?**
 5 A. Yeah, I think... Yeah, as I say
 6 in the e-mail, Fortune top ten. I'm
 7 guessing that's what they were.
 8 **Q. And so the entities listed on the**
 9 **last page of RX-4 represent the top ten**
 10 **hospitals that were the subject of the**
 11 **first phase of your research. Is that fair**
 12 **to say?**
 13 A. Yes, though I'm not sure if this
 14 was our final list. We had also considered
 15 other ways to consider top ten, so I would
 16 have to do a comparison to be sure that
 17 this was in fact the ones we used.
 18 **Q. There is a chart in your report**
 19 **on page 11.**
 20 A. Yup, looks like we got them.
 21 **Q. So the chart on page 11 of RX-3,**
 22 **is it your testimony that the list matches**
 23 **the list of entities listed on the last**
 24 **page of RX-4?**
 25 A. Yup, it appears to.

1 Johnson
 2 **Q. Okay. If we could go back to**
 3 **RX-3, please, page 10. After the mention**
 4 **of the top ten publicly traded health care**
 5 **firms, you indicate that, "...we developed**
 6 **a digital footprint for each health care**
 7 **institution."**
 8 **Do you see that?**
 9 A. Yes.
 10 **Q. What is a digital footprint?**
 11 A. These would be, as it's described
 12 in the paper, terms related to those
 13 institutions.
 14 **Q. So you would develop terms**
 15 **related to each institution?**
 16 A. Yes.
 17 **Q. You go on to say, "...for**
 18 **example, names of the affiliated hospitals,**
 19 **clinics, key brands, et cetera."**
 20 A. Yes.
 21 **Q. So those are the types of terms**
 22 **you would use to search each of these top**
 23 **ten health care firms?**
 24 A. Yes.
 25 MR. SHERMAN: Can we mark this as

1 Johnson
 2 5, please?
 3 (Two-page e-mail string marked
 4 Exhibit RX-5 for identification)
 5 **Q. I've shown you what's been marked**
 6 **as RX-5, and I'll ask you to look at that.**
 7 **Can you tell us what that is,**
 8 **please?**
 9 A. An e-mail between myself and
 10 Chris.
 11 **Q. And it's dated November 19, 2007.**
 12 **Is that correct?**
 13 A. Yup.
 14 **Q. The subject is "Medical probing**
 15 **terms."**
 16 **Do you see that?**
 17 A. Yes.
 18 **Q. And below that, there are some**
 19 **terms.**
 20 **What were these terms used for?**
 21 A. They were added to the digital
 22 footprint that we were using for each of
 23 those top ten organizations.
 24 **Q. So these were not the -- to your**
 25 **recollection, they were not the original**

1 Johnson
 2 **terms that you were using to search; they**
 3 **were additional terms?**
 4 A. Yes, many of which were already
 5 included, in fact, in the original terms,
 6 but we wanted to be sure that we had a good
 7 list.
 8 MR. SHERMAN: Let's look at RX-6,
 9 please. I'm going to show you what's
 10 been marked as RX-6.
 11 (Four-page spreadsheet, first
 12 page being blank, marked Exhibit RX-6
 13 for identification)
 14 **Q. You've been handed what's been**
 15 **marked as RX-6, and I'd ask that you take a**
 16 **look at that, particularly the second page**
 17 **and the fourth page. Can you identify what**
 18 **that is for us, please?**
 19 A. It looks like the contents of a
 20 spreadsheet.
 21 **Q. And if you look at the last page,**
 22 **do you know what that is?**
 23 A. It looks like the metadata
 24 associated with this particular file.
 25 **Q. Would these be search terms that**

1 Johnson
 2 A. There were unique names in each
 3 one and names in common.
 4 **Q. On page 11, near the bottom third**
 5 **of that first paragraph, it says, "...**
 6 **files captured" -- well, let me go back a**
 7 **little further. "Of course, increasing the**
 8 **number of terms included in the digital**
 9 **footprint increased the number file matches**
 10 **found but also [increased] false**
 11 **positives..." What is a false positive?**
 12 A. From our point of view, they were
 13 files unrelated to health care.
 14 **Q. Who made the determination that a**
 15 **file was a false positive?**
 16 A. We did.
 17 **Q. And that would be you and your**
 18 **assistant?**
 19 A. Yes.
 20 **Q. Or you and Tiversa?**
 21 A. The Dartmouth team.
 22 **Q. It goes on to say, "...files**
 23 **captured that have nothing to do with the**
 24 **institution in question." What is meant**
 25 **by "captured"?**

1 Johnson
 2 **were used on page 2 of this particular**
 3 **exhibit?**
 4 A. I don't think so, in this case.
 5 We had considered doing a study in the
 6 insurance industry, but then decided to
 7 focus more squarely on health care.
 8 **Q. I see.**
 9 **So let's go back to RX-3, please.**
 10 **You indicate in the second paragraph under**
 11 **Section 4, "Research Method and Analysis.**
 12 **With the help of Tiversa Inc., we searched**
 13 **P2P networks using our digital signature**
 14 **over a two-week period (in January, 2008)**
 15 **and randomly gathered a sample of shared**
 16 **files related to health care and these**
 17 **institutions." Do you see that?**
 18 A. Yes.
 19 **Q. Did I read it correctly?**
 20 A. Yes.
 21 **Q. So the digital signature is the**
 22 **same as a digital footprint?**
 23 A. Yes.
 24 **Q. Was the digital signature**
 25 **different for each health care firm?**

1 Johnson
 2 A. Ones that were shared that we
 3 were able to observe.
 4 **Q. How was the determination made**
 5 **about which of the captured files that you**
 6 **were able to observe would actually be made**
 7 **available to Dartmouth by Tiversa? Or were**
 8 **all of the captured files made available?**
 9 A. I believe all the captured files
 10 were made available.
 11 **Q. Okay. By one of the three or**
 12 **four ways that we discussed earlier?**
 13 A. Yes, comprising that sample of
 14 3,328 files.
 15 **Q. Under Figure 2 on page 11 of**
 16 **RX-3, you indicate that 50 percent of the**
 17 **3,328 files were considered to be duplicate**
 18 **copies. Is that correct?**
 19 A. Correct.
 20 **Q. And how would you define a**
 21 **"duplicate copy"?**
 22 A. I feel it's self-evident.
 23 **Q. Well, would you tell us for the**
 24 **record, please?**
 25 A. A copy that's the same as the

1 Johnson
 2 other.
 3 **Q. Well, in your report you say that**
 4 **it's, "...the same file...that had spread**
 5 **or were on multiple IP addresses."**
 6 A. Yes.
 7 **Q. So it would not be a copy under**
 8 **the definition used in the article if it**
 9 **were not the same file that had spread or**
 10 **were on multiple IP addresses?**
 11 MS. RIPOSO VAN DRUFF: Objection;
 12 argumentative.
 13 **Q. Correct?**
 14 A. Our technology allowed us not to
 15 retrieve the same file from the same user
 16 multiple times.
 17 **Q. But this seems to be indicating**
 18 **that it was the same file that had spread**
 19 **and was on multiple IP addresses, which**
 20 **would indicate, correct me if I'm wrong,**
 21 **that it's not the same user.**
 22 A. There are cases where it could be
 23 the same user. I may have a file on my
 24 laptop computer and be plugged into a
 25 network at work and receive an IP address

1 Johnson
 2 based on my work network, but then I go to
 3 the hotel and log in using a different ISP
 4 and get a different IP address. Same file;
 5 two different IP addresses.
 6 We couldn't distinguish between
 7 those. We could take -- we would end up
 8 with both of them.
 9 **Q. Were there examples of the same**
 10 **file shared from different sources?**
 11 A. I believe so. But it was not
 12 easy or possible always for us to be able
 13 to tell if they were truly different
 14 sources or just the scenario I described
 15 earlier.
 16 **Q. Was that true in both phases of**
 17 **the study in terms of trying to determine**
 18 **the source of a captured file?**
 19 MS. RIPOSO VAN DRUFF: Objection;
 20 vague.
 21 A. I'm not sure I can answer that
 22 question.
 23 **Q. Maybe we'll come back to it**
 24 **later. It might make more sense.**
 25 You indicate on page 12 in the

1 Johnson
 2 **first sentence of the first full paragraph**
 3 **on that page, "The most common type of the**
 4 **files found were newspaper and journal**
 5 **articles, followed by documents associated**
 6 **with students studying medicine."**
 7 A. Yes.
 8 **Q. Did I read that correctly?**
 9 A. Yes.
 10 **Q. And it's true, then, that those**
 11 **documents were not found to be dangerous or**
 12 **harmful to anyone. Is that correct?**
 13 A. Yes. Well, it depends. If
 14 you're a medical textbook publisher, it's
 15 harmful for you if people are sharing your
 16 textbook.
 17 **Q. Right. I understand.**
 18 Below Figure 3 you indicate that,
 19 "The set of dangerous documents discovered
 20 contained several files that would
 21 facilitate medical identity theft. One
 22 such document was a government application
 23 for employment asking for detailed
 24 background information."
 25 How is that information

1 Johnson
 2 **considered dangerous?**
 3 A. Dangerous in the sense that it
 4 provides personal identifying information
 5 about an individual which they may not wish
 6 to have broadly shared.
 7 **Q. Was the source of this file**
 8 **known?**
 9 A. I don't know.
 10 **Q. Page 13, the first full**
 11 **paragraph, you indicate, "More disturbing,**
 12 **we found a hospital-generated spreadsheet**
 13 **of personally identifiable information on**
 14 **recently-hired employees, including Social**
 15 **Security numbers contract information, job**
 16 **category, etc."**
 17 Did I read that correctly?
 18 A. Yes.
 19 **Q. Now, obviously that's a dangerous**
 20 **document --**
 21 A. Yes.
 22 **Q. -- you would agree?**
 23 A. Yes.
 24 **Q. Did you determine the source of**
 25 **that particular document?**

1 Johnson
 2 MS. RIPOSO VAN DRUFF: Vague as
 3 to "source."
 4 A. The Dartmouth team, the focus of
 5 our research was not sources, so we put
 6 really no effort into trying to determine
 7 the source of any documents described in
 8 this paper.
 9 **Q. Then let's move down to the**
 10 **second full paragraph on page 13, where it**
 11 **reads, "As a second stage of our analysis,**
 12 **we then moved from sampling with a large**
 13 **net to more specific and intentional**
 14 **searches..." Do you see that?**
 15 A. Yes.
 16 **Q. Did I read that correctly?**
 17 A. Yes.
 18 **Q. You would consider using the**
 19 **terms associated with the top ten health**
 20 **care firms, and also creating a digital**
 21 **footprint or a digital signature containing**
 22 **terms associated with those top ten firms,**
 23 **both individually and generally, to be a**
 24 **broader net in terms of searching for**
 25 **potential files to capture?**

1 Johnson
 2 **Dartmouth team's idea to do more specific**
 3 **and intentional searches?**
 4 A. We became aware of LimeWire's
 5 ability to, as we described, follow
 6 specific nodes. It's a functionality that
 7 LimeWire provides its users, because when
 8 you're searching for music and I find that
 9 you have a similar taste in music that I
 10 do, that I may want to see what other songs
 11 you're sharing. So if I search for
 12 Madonna, "Material Girl," and find it on
 13 your computer, I may believe that you have
 14 other songs from Madonna or related songs
 15 to "Material Girl" that I would appreciate.
 16 **Q. Was the second stage of the**
 17 **research done because you were not**
 18 **satisfied with the type of information you**
 19 **had gotten during the first stage and**
 20 **wanted more?**
 21 MS. RIPOSO VAN DRUFF: Objection;
 22 vague as to "satisfied."
 23 A. We certainly were interested in
 24 finding other examples, yes.
 25 **Q. And did you communicate to**

1 Johnson
 2 A. Yes.
 3 **Q. Why?**
 4 A. Because many of those terms are
 5 still vague, not specific, so they would
 6 often uncover many, many unrelated, as we
 7 report, files.
 8 **Q. And so to do a more specific and**
 9 **intentional search, what did you do?**
 10 A. Well, first, I need to qualify
 11 that by the fact that we didn't search, the
 12 Dartmouth team didn't search, any networks
 13 for any files ourself. Tiversa did all the
 14 searching.
 15 And, secondly, to answer your
 16 question, we defined very specifically
 17 exactly what Tiversa did in that step.
 18 **Q. Now, did the Dartmouth team**
 19 **suggest that Tiversa take these steps, or**
 20 **did Tiversa suggest to Dartmouth that these**
 21 **were the steps that needed to be taken to**
 22 **do a more specific and intentional search?**
 23 A. I don't think I can answer that
 24 question.
 25 **Q. The question is: Was it the**

1 Johnson
 2 **Tiversa that you were interested in finding**
 3 **more examples, or did Tiversa indicate to**
 4 **you that you could really find more**
 5 **examples if you did A, B, C?**
 6 A. We communicated to Tiversa that
 7 we were interested in finding more
 8 examples.
 9 **Q. And did they guide you in how you**
 10 **could possibly find more examples?**
 11 MS. RIPOSO VAN DRUFF: Objection;
 12 vague as to "guide."
 13 A. Their own technology that we were
 14 aware of allowed for more searching than we
 15 had done in Phase 1, yes.
 16 **Q. It was a different type of**
 17 **search, correct?**
 18 A. Correct.
 19 **Q. In fact --**
 20 A. That's why we describe it in the
 21 paper.
 22 **Q. In fact, you described the search**
 23 **as, "One of the features enabled by**
 24 **LimeWire and other sharing clients is the**
 25 **ability to examine all the shared files of**

1 Johnson
2 a particular user, (sometimes called
3 'browse host'). Over the next since
4 months, we periodically examined hosts that
5 appeared promising for shared files." Did
6 I read that correctly?

7 A. Yes.

8 Q. How is it determined which browse
9 hosts would be periodically examined over
10 the next six months?

11 A. Very much as I described for
12 music: Posts that had leaked were sharing
13 files that appeared interesting.

14 Q. And so is it fair, then, to say
15 that, consistent with Stage 1, these hosts
16 were affiliated with the top ten health
17 care firms?

18 MS. RIPOSO VAN DRUFF: Objection;
19 misstates prior testimony --

20 A. No.

21 MS. RIPOSO VAN DRUFF: -- vague
22 as to "affiliated."

23 Q. So the hosts did not necessarily
24 need to be affiliated with the top ten
25 health care firms that the broad net was

1 Johnson
2 That sentence suggests that
3 information came from the first sampling,
4 but you're indicating that some of it could
5 have and some of it could not have. Is
6 that right?

7 MS. RIPOSO VAN DRUFF: Objection;
8 misstates prior testimony.

9 A. What we're conveying there is
10 that we learned things in our first sample
11 that helped us.

12 Q. That last paragraph, you indicate
13 that, "Using this approach, we uncovered
14 far more disturbing files. For a medical
15 testing lab, we found a 1,718-page document
16 containing patient Social Security numbers,
17 insurance information, and treatment codes
18 for thousands of patients."

19 Did I read that correctly?

20 A. You did.

21 Q. Is it fair to say that the browse
22 host from which that information was
23 captured, you can't identify who that is?

24 A. I can't.

25 Q. Is it fair to say that the browse

1 Johnson
2 cast --
3 A. No.
4 Q. -- for in the first stage?
5 A. No.
6 Q. Were these hosts users who had
7 leaked files that had been captured during
8 the first stage of the research?
9 A. They could have been.
10 Q. So is it fair to characterize
11 your testimony, then, that the browse hosts
12 that were periodically examined for six
13 months who appeared promising for shared
14 files were not necessarily those that were
15 discovered by virtue of shared files in the
16 first stage?

17 MS. RIPOSO VAN DRUFF: Objection;
18 misstates prior testimony.

19 A. I don't know if I could answer
20 that question. You have to ask Tiversa.

21 Q. So let's go one sentence before
22 the last one I just read, where it
23 says, "Using information from the first
24 sampling, we examined shared files on hosts
25 where we had found other dangerous data."

1 Johnson
2 host whose file that information was
3 captured from, you don't know whether or
4 not that browse host was identified in the
5 first stage of the research?

6 A. I don't know.

7 Q. Do you know when you received
8 this particular file from Tiversa?

9 A. I know the time frame. It's the
10 time frame described in the paper. The
11 exact date, we could look, look it up.

12 Q. When did the -- I understand that
13 during the first stage there were two weeks
14 in January of...

15 A. 2008.

16 Q. 2008 -- thank you -- where the
17 first stage was conducted. When did the
18 sixth month period begin for the second
19 stage?

20 A. It began shortly thereafter and
21 continued into the summer.

22 Q. So is it fair to say that there
23 was no large gap of weeks between the first
24 stage and the second stage?

25 A. There may have been weeks.

61

1 Johnson
 2 **Q. How many? Do you know?**
 3 A. I don't. I don't recall.
 4 **Q. Not more than a month of weeks?**
 5 A. It could have been a month.
 6 **Q. It could have been a month.**
 7 **Could it have been longer than two months?**
 8 A. Potentially. Not longer than
 9 six.
 10 **Q. Not longer than six months.**
 11 MR. SHERMAN: If we could mark
 12 this as 7.
 13 (Three-page e-mail chain marked
 14 Exhibit RX-7 for identification)
 15 **Q. I've handed you what's been**
 16 **marked as RX-7. Please look at these pages**
 17 **and let me know when you've reviewed them.**
 18 A. I'm reading it backwards. I'm
 19 sorry.
 20 (Pause)
 21 Okay.
 22 **Q. If we start it at the back, is it**
 23 **fair to say that this is a series of**
 24 **e-mails between yourself and Chris Gormley?**
 25 A. Yes.

62

1 Johnson
 2 **Q. And if you – well, these e-mails**
 3 **start on April 29, 2008. Is that correct?**
 4 A. Yes.
 5 **Q. In the middle of the page it**
 6 **says, "Eric, Medical is a treasure-trove of**
 7 **information, but it's not necessarily**
 8 **coming from big hospitals. We've got tons**
 9 **of individual practitioners (most notably**
 10 **psychiatrists) who disclose (since they**
 11 **write up their findings). I'd like to give**
 12 **you a quick call regarding the info -**
 13 **what's your number? I can't find your card**
 14 **right now." Did I read that correctly?**
 15 A. Yes.
 16 **Q. At what stage was the research in**
 17 **April 29, 2008? Does this give you some**
 18 **context as to where you were in the**
 19 **research during that period of time?**
 20 MS. RIPOSO VAN DRUFF: Objection;
 21 vague as to "research."
 22 A. Well, as you can see in the
 23 subsequent e-mail, we're talking about the
 24 process of reviewing the files that we had
 25 found in Phase 1.

63

1 Johnson
 2 **Q. Well, it says, "We are coming**
 3 **well on the medical files - finished going**
 4 **through all of the files. We are working**
 5 **on the report right now. We turned up some**
 6 **interesting stuff..."**
 7 **Is it your testimony that this**
 8 **was a conversation you were having about**
 9 **the files that were captured during**
 10 **Phase 1?**
 11 A. Yes.
 12 **Q. Okay. And you go on to say, "Any**
 13 **chance you could share a couple other of**
 14 **your recent medical finds that we could use**
 15 **to spice up the report? You told me about**
 16 **the one database your found that could**
 17 **really boost the impact of the report.**
 18 **Certainly will coordinate with you on the**
 19 **report and release. I forgot to ask - did**
 20 **you guys also grab searches related to our**
 21 **digital signature?" Did I read that**
 22 **correctly?**
 23 A. Yes.
 24 **Q. Based on your review of these**
 25 **communications set out in RX-7, would it be**

64

1 Johnson
 2 **fair to say that this was prior to Stage 2**
 3 **of the research?**
 4 A. No.
 5 **Q. Okay. Would it be fair to say**
 6 **that this was prior to your getting any**
 7 **results from Phase 2 of the research?**
 8 A. No.
 9 **Q. Okay.**
 10 A. As we discussed in this e-mail,
 11 we had already been talking about Phase 2.
 12 **Q. Well, where in these e-mails do**
 13 **you see a mention of Phase 2?**
 14 A. Further files that Tiversa was
 15 finding.
 16 **Q. Okay.**
 17 **Had you received any of those**
 18 **files?**
 19 A. No.
 20 **Q. The last sentence that's found on**
 21 **page 2, it says, "Did you guys also grab**
 22 **searches related to our digital signature?"**
 23 A. Yes.
 24 **Q. Do you see that?**
 25 A. Yes.

1 Johnson
 2 Q. Was the digital signature used in
 3 Phase 1 and Phase 2?
 4 A. Phase 1.
 5 Q. Phase 1.
 6 And when you state, "You told me
 7 about the one database you found that could
 8 really boost the impact of the report," is
 9 it correct to assume that through verbal or
 10 e-mail communications you had been told
 11 about a database that had been found by
 12 Tiversa?
 13 A. Yes.
 14 Q. And if we turn to page 15 of
 15 RX-3, that paragraph is talking about a
 16 hospital where we found two spreadsheet
 17 databases. Is this the same database that
 18 was referenced in your e-mail of April 29,
 19 2008?
 20 A. Possibly.
 21 Q. Possibly.
 22 If you look at the last sentence
 23 above Figure 5 on page 15 -- well, it's the
 24 next-to-the-last sentence. It says, "In
 25 this case, the hemorrhage came from an

1 Johnson
 2 outsourced collection agency working for
 3 the hospital."
 4 Now, you testified earlier that
 5 it wasn't the focus to identify sources.
 6 But this is a source that was identified.
 7 Is that correct?
 8 A. Yes.
 9 Q. Why was this particular source
 10 identified?
 11 A. It was possible. Sources weren't
 12 always possible.
 13 Q. Oh.
 14 A. Sometimes it was self-evident
 15 from the file.
 16 Q. So what you're saying is, based
 17 on the information it was clear where this
 18 file came from?
 19 A. Yes.
 20 Q. And at other times, the
 21 information on the captured files was not
 22 so easily discernible as to where it came
 23 from?
 24 A. Yes.
 25 Q. I may have asked you this, and I

1 Johnson
 2 apologize if I have: Who determined which
 3 browser host was going to be monitored for
 4 six months?
 5 A. Tiversa.
 6 Q. You had mentioned that the
 7 network is constantly changing --
 8 A. Yes.
 9 Q. -- expanding, contracting. Is
 10 that because there are, at any given time,
 11 a different number of users on a particular
 12 network that's being searched?
 13 A. Yes.
 14 (Six-page double-sided e-mail
 15 string, Bates stamped Eric Johnson -
 16 000001 and 2, 21 and 22, and 27 through
 17 34, marked Exhibit RX-8 for
 18 identification)
 19 Q. I've handed you what's just been
 20 marked as RX No. 8, and I'll ask that you
 21 take a look at that and let me know when
 22 you've reviewed it.
 23 MS. RIPOSO VAN DRUFF: Counsel,
 24 may I just ask, the Bates skips from
 25 21 -- excuse me, from 2 to 22. Is that

1 Johnson
 2 deliberate?
 3 MR. SHERMAN: This is deliberate
 4 because the report, the "Data
 5 Hemorrhaging" report, was in between
 6 that.
 7 MS. RIPOSO VAN DRUFF: Okay. And
 8 then it skips to 27. That is also
 9 deliberate?
 10 MR. SHERMAN: Yes, maybe what
 11 was. I don't know.
 12 MR. O'LEARY: I think his résumé,
 13 maybe, was in there.
 14 MR. SHERMAN: Yes, it was
 15 something that wasn't e-mails.
 16 MR. O'LEARY: I think in my cover
 17 letter I laid out some of the numbering
 18 challenges we had, since we were
 19 relatively new at it.
 20 Q. In RX-8, the first page is an
 21 e-mail from Carl Settlemeyer to you dated
 22 February 3, 2009. Is that correct?
 23 A. Yes.
 24 Q. And he's requesting a copy of the
 25 article. And the article is the "Data

1 Johnson
 2 **Hemorrhaging" article. Is that correct?**
 3 A. Yes.
 4 **Q. On page 2, your response to**
 5 **Mr. Settlemyer is, "Yes Carl, I remember**
 6 **you."**
 7 **Do you see that?**
 8 A. Yes.
 9 **Q. Where do you remember**
 10 **Mr. Settlemyer from?**
 11 A. I believe we met in and around
 12 the time that I testified related to our
 13 work in banking.
 14 **Q. And where did you testify in**
 15 **relation to your work in banking?**
 16 A. House committee.
 17 **Q. And what year was that?**
 18 A. Possibly 2006, but I'm not
 19 certain. I would have to go look.
 20 **Q. After your testimony you**
 21 **indicated you met Mr. Settlemyer. Did you**
 22 **have subsequent conversations with**
 23 **Mr. Settlemyer other than what's located**
 24 **here in these e-mails?**
 25 A. Not that I recall.

1 Johnson
 2 **Q. If I look at page 22, it's**
 3 **another e-mail from Mr. Settlemyer to you**
 4 **dated February 3rd. And he indicates, "We**
 5 **have greatly appreciated your insights into**
 6 **your work in the past."**
 7 **Does that refresh your**
 8 **recollection as to whether or not there**
 9 **were other conversations with**
 10 **Mr. Settlemyer about your work?**
 11 MS. RIPOSO VAN DRUFF: Objection;
 12 asked and answered.
 13 A. I think he's referring to the
 14 work on banking.
 15 **Q. Were there any conversations**
 16 **between you and Mr. Settlemyer about your**
 17 **work on banking?**
 18 A. At some point we had a
 19 conversation in and around the time of that
 20 house testimony.
 21 **Q. Was it before or after the**
 22 **testimony?**
 23 A. I would say after, but I'm not
 24 certain.
 25 **Q. If you'll look down on page 22 as**

1 Johnson
 2 **well, it's an e-mail from you to**
 3 **Mr. Settlemyer. You indicate, "...leakage**
 4 **in the health care sector is more complex**
 5 **and (in some ways) frightening."**
 6 **What do you mean by "leakage in**
 7 **the health care sector is more complex"?**
 8 **And I suspect that you're comparing it to**
 9 **leakage in the financial sector?**
 10 A. Correct. The types of data, the
 11 fact that the data may be personal
 12 identifiable data, like in banking, data
 13 that would be used to commit traditional
 14 financial fraud or financial identity
 15 theft, but also data that is much more
 16 personal in nature and could be used in
 17 many other ways.
 18 **Q. So you described in your answer**
 19 **just now that the data was more complex. I**
 20 **actually took the sentence meaning that the**
 21 **leakage was more complex. Was that an**
 22 **incorrect way to interpret that sentence?**
 23 A. I think my meaning there was the
 24 data itself. There may have been, in my
 25 mind, some idea of the fragmented nature of

1 Johnson
 2 health care, which is different than
 3 banking, meaning that there are many more
 4 small health care establishments.
 5 **Q. If you'll turn to page 27, that's**
 6 **an e-mail from Mr. Settlemyer to you dated**
 7 **March 5, 2009, thanking you for sending the**
 8 **article and indicating that, "We'd like to**
 9 **discuss your research with you when you**
 10 **have...free time."**
 11 MR. SHERMAN: Off the record,
 12 please.
 13 (Off the record)
 14 **Q. Were there discussions about your**
 15 **research with Mr. Settlemyer and Mr. Sheer?**
 16 A. I believe I did have a
 17 conversation with them after this e-mail.
 18 **Q. Did you only have one**
 19 **conversation with them?**
 20 A. There may have been more than
 21 one, but it was no more than one or two.
 22 **Q. The subject matter of the**
 23 **conversations, were they basically focused**
 24 **in on your report?**
 25 A. And my research in this area.

73

1 Johnson
 2 **Q. And your research in the area.**
 3 **Did you exchange any documents**
 4 **with them, with the FTC?**
 5 A. I think this paper, which is
 6 referenced in this e-mail.
 7 **Q. That's the only document you**
 8 **shared with them?**
 9 A. That's the only one I recall
 10 sharing with the FTC.
 11 **Q. If you'll look at the last page**
 12 **of RX-8 -- well, it's the next-to-the-last**
 13 **page, actually, because the pages are two**
 14 **sided. It's an e-mail from Carl Settlemyer**
 15 **to you dated December 8, 2010. It**
 16 **indicates, "You and I have had several**
 17 **conversations in the past about the**
 18 **availability of sensitive information on**
 19 **P2P file-sharing networks. Would you have**
 20 **some time on Thursday or Friday to speak**
 21 **with me briefly about some potential work**
 22 **we may have for you on that subject?"**
 23 **What was the potential work that**
 24 **they had for you on the subject?**
 25 A. At that time, I recall the FTC

74

1 Johnson
 2 was interested in building educational
 3 material for the general public on the
 4 dangers of file sharing, and I think on
 5 that phone call, they -- we discussed the
 6 possibility of participating in the
 7 creation of that educational material.
 8 **Q. Was there any discussion of LabMD**
 9 **or the 1,718-page file that you found from**
 10 **them?**
 11 A. Not that I recall.
 12 **Q. Did you participate with the FTC**
 13 **in creating informational or educational**
 14 **materials for the public?**
 15 A. No.
 16 MR. SHERMAN: Let's take a
 17 ten-minute break.
 18 MS. RIPOSO VAN DRUFF: Sure.
 19 (Recess)
 20 (Two-page double sided
 21 confidentiality agreement, Bates
 22 stamped Eric Johnson - 000023 through
 23 26, marked Exhibit RX-9 for
 24 identification)
 25 EXAMINATION CONTINUED

75

1 Johnson
 2 BY MR. SHERMAN:
 3 **Q. Dr. Johnson, you've just been**
 4 **handed what's been marked as RX-9. Please**
 5 **take a look at that and let me know when**
 6 **you've reviewed it.**
 7 A. Yeah, ready.
 8 **Q. If you'll go to page 24 of RX-9,**
 9 **this appears to be a confidentiality**
 10 **agreement, or at least an unsigned**
 11 **confidentiality agreement, between Tiversa**
 12 **and yourself. Is that correct?**
 13 A. Yes.
 14 **Q. Was this ever executed?**
 15 A. I believe so.
 16 **Q. And was this in connection with**
 17 **the research that we discussed early on in**
 18 **the deposition here today?**
 19 A. It was put in place prior to our
 20 original work with them in 2005, somewhere
 21 in there.
 22 **Q. Okay. And does this refresh your**
 23 **recollection that at least as early as 2005**
 24 **you were working with Tiversa?**
 25 A. Yes.

76

1 Johnson
 2 **Q. If you'll look at Paragraph 3(a),**
 3 **it indicates that you were permitted to**
 4 **disclose confidential information to your**
 5 **employer and other representatives, but**
 6 **only to the extent it was reasonably**
 7 **necessary in order for you to evaluate the**
 8 **technology.**
 9 MS. RIPOSO VAN DRUFF: I'm sorry,
 10 Counsel, did you read that as
 11 "employer" or "employee"?
 12 MR. SHERMAN: I probably said
 13 "employer," but it does say
 14 "employees."
 15 **Q. But only to the extent reasonably**
 16 **necessary in order for you to evaluate the**
 17 **technology.**
 18 **Did you do any formal evaluation**
 19 **of Tiversa's technology?**
 20 A. Yes.
 21 **Q. And what did that evaluation**
 22 **consist of?**
 23 A. We conducted a series of
 24 experiments to determine if in fact they
 25 were able to discover files, as they

1 Johnson
 2 claimed.
 3 Q. And when you say "we," is that a
 4 team of individuals from Dartmouth?
 5 A. Yes.
 6 Q. And so what was the process of
 7 evaluating? Did you search for specific
 8 files, or did you search in specific
 9 business sectors? How was the evaluation
 10 done?
 11 A. We ourselves created files which
 12 we then distributed to users in other
 13 places of the country and world who would
 14 subsequently make those files available
 15 through a file-sharing network. And then
 16 we instructed Tiversa to find those files.
 17 Q. What information did you give
 18 Tiversa in order for them to find the
 19 files?
 20 A. Search strings.
 21 Q. And how specific were the search
 22 strings?
 23 A. They were specific.
 24 Q. Can you describe how specific, or
 25 give me an example of a file that was

1 Johnson
 2 created and shared via a P2P network, and
 3 then certain information given to Tiversa
 4 for them to find that file?
 5 A. The name of the file, parts of
 6 the name or name of the file. I think --
 7 my recollection is we gave them the name of
 8 the file, but...
 9 (Two-page e-mail string marked
 10 Exhibit RX-10 for identification)
 11 Q. You've been handed what's been
 12 marked as RX-10. Please review that and
 13 let me know when you're ready to testify
 14 about it.
 15 A. I'm ready.
 16 Q. RX-10 appears to be -- or it
 17 contains an e-mail at the bottom of the
 18 first page from Samuel Hopkins to yourself,
 19 Keith Tagliaferri, and Griffin Schultz. Is
 20 that correct?
 21 A. Yes.
 22 Q. It's dated March 18, 2008?
 23 A. Yes.
 24 MS. RIPOSO VAN DRUFF: I'm sorry,
 25 Counsel, did you say that that e-mail

1 Johnson
 2 was directed to Dean Johnson?
 3 MR. SHERMAN: I'm sorry, I did.
 4 And it's actually directed to Chris
 5 Gormley, Tagliaferri, and Griffin
 6 Schultz.
 7 Q. Do you know who those people are?
 8 A. They're Tiversa employees.
 9 Q. Do you know what Mr. Hopkins is
 10 referring to when he says, "I'm done with
 11 Dartmouth"?
 12 A. I think he was referring to a
 13 file collection process.
 14 Q. Would that be for the first
 15 phase?
 16 A. I believe that's likely that's
 17 what he's referring to there. I'm not
 18 certain. It wasn't written to me.
 19 Q. It appears that it was
 20 subsequently sent to you, however, by
 21 Mr. Gormley on March 18, 2008.
 22 MS. RIPOSO VAN DRUFF: Objection;
 23 lacks foundation.
 24 A. March -- it looks like March.
 25 Q. March 18th?

1 Johnson
 2 A. I'm looking at my reply, the
 3 26th, but possibly.
 4 Q. In the middle of the page there
 5 is a --
 6 A. Sometime in March.
 7 Q. In the middle of the page there
 8 is a "From" and "To" -- "From," "Sent,"
 9 "To," and "Subject" line. "From" is Chris
 10 Gormley of Tiversa, and "To" is yourself.
 11 Is that correct?
 12 A. Yes.
 13 Q. Dated March 18, 2008?
 14 A. Yes.
 15 Q. And your response, however, at
 16 the top was sent March 26, 2008. Is that
 17 right?
 18 A. Yes.
 19 Q. And it's your belief that this is
 20 referencing documents captured during
 21 Phase 1 of -- or Stage 1 of the research on
 22 data hemorrhaging?
 23 A. Yes.
 24 Q. Are you aware of whether Tiversa
 25 was paid for allowing Dartmouth to use its

1 Johnson
 2 **technology for this research?**
 3 A. We did not have any financial
 4 relationship with Tiversa.
 5 Q. From 2005 through --
 6 A. Ever.
 7 Q. -- through the present?
 8 A. Yes.
 9 Q. Do you know what was in it for
 10 Tiversa to allow you to use this
 11 technology?
 12 MS. RIPOSO VAN DRUFF: Objection;
 13 speculation, vague as to "in it."
 14 A. We were research partners, as you
 15 can see, and they valued the time we spent
 16 conducting the research.
 17 Q. All right.
 18 A. As you might also notice, we
 19 weren't very high on their priority list of
 20 things to do because there's some gaps in
 21 time here.
 22 Q. Is Tiversa mentioned in each
 23 published article in which they --
 24 A. Yes.
 25 Q. -- assisted?

1 Johnson
 2 **Is there an internal review board**
 3 **at Dartmouth for research projects like the**
 4 **ones you've been doing with Tiversa?**
 5 A. There is a committee on the
 6 protection of human subjects.
 7 Q. And that's the only internal
 8 review of research projects that Dartmouth
 9 has in place to review research subjects
 10 that its professors take on?
 11 A. There are other reviews of
 12 faculty members and their research
 13 productivity, but of projects themselves,
 14 the tenets of academic freedom give faculty
 15 wide range of the research subjects they
 16 choose.
 17 Q. Were the funding sources for the
 18 research made aware of Tiversa's
 19 participation in the research?
 20 A. Yes.
 21 Q. And your communication and
 22 involvement with Tiversa is ongoing because
 23 you have current communication in the
 24 research in which they're involved?
 25 MS. RIPOSO VAN DRUFF: Objection;

1 Johnson
 2 misstates prior testimony.
 3 A. No.
 4 Q. Are you aware of whether Tiversa
 5 has an ongoing research partnership with
 6 Dartmouth?
 7 A. No.
 8 Q. You're not aware?
 9 A. Not aware.
 10 Q. So what was the last research
 11 project that you did with Tiversa?
 12 A. There was a subsequent project in
 13 2009 that may have continued into 2010.
 14 I'd have to check my records, but certainly
 15 not within the last couple of years.
 16 (Four-page excerpt from
 17 "Information Governance; Flexibility
 18 and Control Through Escalation and
 19 Incentives," dated April 24, 2008,
 20 marked Exhibit RX-11 for
 21 identification)
 22 Q. Dr. Johnson, you've been handed
 23 what's been marked as RX-11, and I ask if
 24 you recognize that?
 25 A. Yes.

1 Johnson
 2 Q. What is that?
 3 A. It appears to be a working paper,
 4 or part of a working paper.
 5 Q. I will submit for the record that
 6 this paper was 30 pages long, and I
 7 provided an excerpt here of the first four
 8 pages. But you do recognize it as a paper
 9 on which you are listed as a co-author or
 10 co-contributor?
 11 A. Yes.
 12 Q. And this paper was about
 13 information governance. It's entitled
 14 "Information Governance: Flexibility and
 15 Control Through Escalation and Incentives."
 16 Is that correct?
 17 A. Yes.
 18 Q. And April 24, 2008, is that the
 19 publication date?
 20 A. This appears to be a working
 21 paper.
 22 Q. And what is --
 23 A. So this --
 24 Q. What is a working paper?
 25 A. This would be a pre-publication

1 Johnson
2 version of a paper that was not probably
3 complete at that time, though I could check
4 the dates to determine if that were true.
5 **Q. I want to turn you to page 3 of**
6 **the paper. And in the first full paragraph**
7 **on that page there's mention of "the rule**
8 **of least access."**

9 Can you define what the rule of
10 least access is? And I know it may say
11 what it is in the paper, but could you
12 testify to what it is for us, please?

13 A. The idea is that within an
14 organization, that employees are given
15 access to information based on the needs of
16 their jobs but are not provided information
17 beyond those needs.

18 **Q. At the time this research was**
19 **being done, was that a widely-acceptable**
20 **practice of organizations, that you were**
21 **aware of, in terms of information**
22 **governance?**

23 MS. RIPOSO VAN DRUFF: Objection;
24 vague as to "widely acceptable," calls
25 for an expert opinion.

1 Johnson
2 A. If you notice, in the paper we
3 reference other work describing the rule of
4 least access.

5 **Q. Have you done any research in**
6 **terms of how widely used this rule of least**
7 **access is being applied, or was being**
8 **applied, in various business sectors at**
9 **that particular time?**

10 A. No, I hadn't done any research on
11 how widely used the rule of least access
12 was at that time.

13 **Q. Do you think that the rule of**
14 **least access is beneficial to organizations**
15 **who have information that they want to**
16 **protect from inadvertent sharing or sharing**
17 **intentionally?**

18 A. It can be. It depends on the
19 circumstances and need of the employees for
20 the information.

21 **Q. So if an employee needs the**
22 **information to do their job, they should be**
23 **given access to that information. Is that**
24 **correct?**

25 A. That's correct.

1 Johnson
2 **Q. And if they don't need it to do**
3 **their job, then the rule of least access**
4 **suggests that they should not be given**
5 **access to that information?**

6 A. That's correct. However, as we
7 describe in this paper, there are many
8 areas in between.

9 **Q. Yes.**
10 **On page 4, second sentence of the**
11 **first full paragraph it states, "For**
12 **example, all tellers in a bank perform**
13 **roughly the same job and receive the same**
14 **set of privileges. This approach works**
15 **well for organizations with a few dominant**
16 **roles that do not change."**

17 **Did I read that correctly?**

18 A. Yes.

19 **Q. So, paraphrasing, is it fair to**
20 **say that the rule works well in those**
21 **organizations where a group of people**
22 **perform roughly the same function and**
23 **therefore are given access to the same**
24 **information?**

25 MS. RIPOSO VAN DRUFF: Objection

1 Johnson
2 to form; misstates prior testimony.
3 And I further object to the extent that
4 the witness does not have a complete
5 copy of this working paper that appears
6 in excerpted form of RX-11.

7 A. In that paragraph, we're
8 describing role-based access, which often
9 employs concepts from the rule of least
10 access. But role based, as indicated in
11 that paragraph, segments employees into
12 roles, and then in that role they're given
13 a set of privileges, which is uniform
14 across that role. It may not always be the
15 case that that is the least access needed
16 by every individual in that role.

17 **Q. So it's fair to say that the**
18 **least access rule starts out generally, and**
19 **then it can be tailored to the needs of the**
20 **organization that is applying it?**

21 MS. RIPOSO VAN DRUFF: Objection
22 to form; misstates prior testimony.

23 A. The least access rule in
24 implementation would drive the necessity
25 for each individual in the organization to

1 Johnson
 2 have specifically-tailored access policies.
 3 Role-based puts individuals into groups
 4 where they share the same access in that
 5 role.
 6 MR. SHERMAN: Okay. If we take
 7 like a five-minute break, I may be
 8 finished.
 9 MS. RIPOSO VAN DRUFF: Certainly.
 10 Thank you, William.
 11 (Recess)
 12 EXAMINATION CONTINUED
 13 BY MR. SHERMAN:
 14 Q. A couple of more questions.
 15 Let's look at RX-3, which is your
 16 "Data Hemorrhaging."
 17 A. Yes.
 18 Q. On page 19 you indicate that,
 19 "Coupled with the portability of data,
 20 inadvertent disclosures are inevitable."
 21 And I guess you're coupling that with,
 22 "information access within many health care
 23 systems is lax and the need for better
 24 monitoring and information controls to
 25 detect and symptom leaks." Is that

1 Johnson
 2 correct?
 3 A. Yes.
 4 Q. So I guess that you're not saying
 5 that -- well, what are you saying? What
 6 are you saying? Are you saying that it's
 7 inevitable that some information is going
 8 to get out?
 9 A. Yes.
 10 Q. That because there's no perfect
 11 security?
 12 A. I believe that's true today.
 13 Q. So if an organization had the
 14 latest technology, written policies, rules,
 15 procedures, is it your position that it
 16 would be inevitable that some information
 17 would get out if someone wanted to get it?
 18 MS. RIPOSO VAN DRUFF: Objection;
 19 incomplete hypothetical, calls for an
 20 expert opinion.
 21 A. There's a broad difference
 22 between what we discuss in this paper as
 23 inadvertent disclosure versus an active
 24 hacker. I do believe that inadvertent
 25 disclosures can be controlled and managed.

1 Johnson
 2 Preventing every type of hacker is more
 3 troublesome.
 4 Q. What about, for lack of a better
 5 word, an ill-intended employee?
 6 A. We call those insider --
 7 MS. RIPOSO VAN DRUFF: I'm sorry,
 8 to interrupt, but objection. It's an
 9 incomplete hypothetical, and it calls
 10 for an expert opinion.
 11 Q. You call those?
 12 A. An insider.
 13 Q. Yes, an insider. Are there any
 14 perfect security measures that can be taken
 15 against insiders?
 16 MS. RIPOSO VAN DRUFF: Objection;
 17 incomplete hypothetical, calls for an
 18 expert opinion.
 19 A. There certainly are many measures
 20 that firms can take. Perfect, that's
 21 another challenge.
 22 MR. SHERMAN: Okay. I have no
 23 further questions.
 24 MS. RIPOSO VAN DRUFF: Before we
 25 go off the record, I just want to state

1 Johnson
 2 that to the extent that respondent
 3 counsel wishes to use RX-11 at any
 4 point further in this proceeding,
 5 complaint counsel objects because it is
 6 an incomplete document. And if we can
 7 go off the record, please.
 8 (Off the record)
 9 EXAMINATION
 10 BY MS. RIPOSO VAN DRUFF:
 11 Q. Good afternoon, Dean Johnson. I
 12 introduced myself to you this morning, but
 13 my name is Laura VanDruff and I am an
 14 attorney with the Federal Trade Commission.
 15 Today, I'm serving in the role as complaint
 16 counsel in the matter of LabMD. With me
 17 today is my colleague Alain Sheer.
 18 Before this morning, have we met,
 19 Professor Johnson?
 20 A. No.
 21 Q. Have we spoken before?
 22 A. No.
 23 Q. Prior to the research that led
 24 to --
 25 MS. RIPOSO VAN DRUFF: Well, for

1 Johnson
2 the benefit of the record I am going to
3 mark as CX0382 a document, an identical
4 copy of which appears as RX-3. This is
5 for our housekeeping, because the judge
6 wants unique exhibit numbers for every
7 document.

8 MR. O'LEARY: Could I just say
9 that it's actually not an exact
10 duplicate of RX-3 because of what's
11 included at the back of RX-3, which I
12 think is our error. But the first
13 pages, you know, 3 through 21, are the
14 same as RX-3.

15 MS. RIPOSO VAN DRUFF: Thank you
16 for that clarification.

17 Q. Dean Johnson, for the benefit of
18 the record, may I ask you to please
19 identify the document that I have now
20 replaced that appears at CX382?

21 A. Yes.

22 Q. What is the document that appears
23 at 382?

24 A. It's a paper that we presented at
25 the Financial Crypto and Data Security

1 Johnson
2 Q. Has any government agency ever
3 directed you to search for documents that
4 were created by LabMD?

5 A. No.

6 Q. Has any government agency ever
7 predicated its funding of your research on
8 you finding customer information obtained
9 by LabMD?

10 A. No.

11 Q. Did the Federal Trade Commission
12 or its staff contribute in any way to the
13 research that resulted in the paper that
14 appears at CX382?

15 A. No.

16 Q. Did the Federal Trade Commission
17 or its staff ever review a draft of the
18 manuscript that resulted in the paper that
19 appears at CX382 before it was finalized
20 for publication?

21 A. No.

22 Q. Dean Johnson, do you have an area
23 of interest on which you focus your
24 research?

25 A. Information technology.

1 Johnson
2 Conference in February of 2009.
3 Q. And is it a complete copy of that
4 paper?
5 A. Yes.
6 Q. Prior to the research that led to
7 the paper that's been marked as CX382, have
8 you ever heard of LabMD?

9 A. No.

10 Q. Had you ever heard of
11 Mr. Daughterty?

12 A. No.

13 Q. And the research that led to the
14 paper that has been marked as CX382, were
15 you specifically looking for documents that
16 related to LabMD?

17 A. No.

18 Q. Were you specifically looking for
19 the sensitive personal information of
20 LabMD's customers?

21 A. No.

22 Q. Have you ever conducted research
23 in which you specifically looked for
24 documents from LabMD?

25 A. No.

1 Johnson
2 Q. Did your work at HP contribute to
3 that area of interest?

4 A. Yes.

5 Q. How did it contribute?

6 A. We were developing information
7 systems to run factories.

8 Q. Have you prepared similar
9 articles regarding the risk to corporations
10 and to individuals created by the
11 inadvertent disclosure of consumers'
12 personal information?

13 A. Yes.

14 Q. Have those articles been
15 published in peer-reviewed literature?

16 A. Yes.

17 Q. Have you presented at national
18 academic conferences?

19 A. Yes.

20 Q. Have you testified before
21 Congress?

22 A. Yes.

23 Q. Did you develop a particular
24 interest in P2P file sharing?

25 A. Yes.

1 Johnson

2 Q. And why is that?

3 A. Because it allows an unusual view
4 into the problems of inadvertent
5 disclosure.

6 Q. And what do you mean by "an
7 unusual view"?

8 A. Well, as we describe in our
9 papers, there are many different ways that
10 information can be inadvertently disclosed.
11 For example, if I lose my laptop on the
12 train, or if I put something on the flash
13 drive and then forget it at the cleaners,
14 those in fact become inadvertent
15 disclosures.

16 But they're more challenging to
17 study, particularly in the broader sense.
18 And we chose to study inadvertent
19 disclosures in peer-to-peer file sharing
20 because it allowed us the opportunity to
21 see the kinds of files that could be
22 inadvertently disclosed.

23 Note that the same files that get
24 lost on a laptop are the same files that
25 often are disclosed in peer-to-peer file

1 Johnson

2 Q. And have they been published by
3 peer-reviewed journals?

4 A. Yes.

5 Q. I'd like you to direct your
6 attention to the document that's been
7 marked as CX382, a copy of the "Data
8 Hemorrhaging" paper, and specifically to
9 the page that appears at Bates 0000010. In
10 the first full paragraph, the third line
11 describes P2P users copying files that have
12 been exposed.

13 What is the risk to a sensitive
14 file after it has been exposed on a P2P
15 network?

16 A. That file faces the risk that
17 someone wishing to exploit its contents
18 would be able to retrieve it.

19 Q. Is there also a risk that it will
20 be saved by someone other than the user
21 from whom the file was originally taken?

22 A. Yes.

23 Q. Is there a risk that a sensitive
24 file will be re-shared on a P2P network?

25 A. Yes.

1 Johnson

2 sharing. And thereby, peer-to-peer file
3 sharing for us was really more of a place
4 that allowed us to study a much broader
5 problem.

6 Q. And the broader problem is what?

7 A. Inadvertent disclosure.

8 Q. Earlier today you described for
9 Mr. Sherman how P2P technology works. Do
10 you remember that testimony?

11 A. Yes.

12 Q. How did you develop that
13 understanding?

14 A. I developed that understanding in
15 the conduct of this research, though I will
16 be quick to say that I'm not an expert in
17 that technology.

18 Q. But have you designed experiments
19 to track the movement of consumer
20 information across P2P networks?

21 A. Yes.

22 Q. And have those experiments been
23 reviewed by the editorial boards of
24 peer-reviewed journals?

25 A. Yes.

1 Johnson

2 Q. Describe that risk.

3 MR. SHERMAN: Objection; vague.
4 You may answer.

5 A. Files that are shared on P2P
6 networks are often viewed and used by
7 others who then re-share them. And it's a
8 concept that we coined "the digital wind,"
9 the idea that as soon as the files are made
10 available, they, like a newspaper blowing
11 in the wind, they seem to blow around.
12 But, unlike digital wind, as they blow they
13 seem to multiply.

14 Q. What do you mean by "multiply"?

15 A. You have multiple instances of
16 the same file on different user accounts.

17 Q. And how does that affect the
18 likelihood that a sensitive file may be
19 misused?

20 A. It increases the likelihood.

21 Q. Do the materials shared on P2P
22 networks vary from day to day?

23 A. Yes.

24 Q. Why is that?

25 A. Because users are constantly

101

1 Johnson
 2 joining and leaving the network, so at any
 3 point in time, the number of users on the
 4 network is changing. And, in fact, what
 5 the users may be sharing is also changing.
 6 Q. So if I were to search for a
 7 particular document by its title today and
 8 I did not find it, what conclusions could I
 9 draw about the document's availability on a
 10 P2P network?

11 MR. SHERMAN: Objection; calls
 12 for speculation. You may answer.

13 A. You couldn't conclude anything.

14 Q. Why not?

15 A. There are two reasons: one is
 16 that the individual may not be
 17 participating in the network at that time;
 18 and, second, that you may not have found
 19 the file, even if the user is participating
 20 in the network at that time.

21 Q. And under what circumstances
 22 would I not find the file if the user were
 23 participating in the network at that time?

24 A. If that user were distant from
 25 you in the network -- "distant" meaning

103

1 Johnson
 2 attention, please, to the document that I
 3 marked as CX382. This is the "Data
 4 Hemorrhaging" paper. And I would ask you
 5 to turn to the page that's been Bates
 6 labeled 14.

7 On page 14 appears Figure 4.
 8 What is Figure 4?

9 A. Figure 4 is an insurance aging
 10 report. It's a screenshot of a redacted
 11 page from that report.

12 Q. Is this an excerpt of a LabMD
 13 document?

14 A. I believe it is an excerpt from a
 15 LabMD document.

16 Q. How do you know?

17 A. The portion that was redacted at
 18 the top indicated that it was LabMD.

19 Q. And you know that because you
 20 performed the redaction?

21 A. Yes, we performed the redaction
 22 to publish it.

23 Q. And I direct your attention to
 24 the preceding page of Bates 13.

25 In the last paragraph that

102

1 Johnson
 2 that there were many people between you and
 3 them -- your search may never reach them.
 4 Q. And if I, in 2008, were to search
 5 for a particular document by its title and
 6 did not find it, what conclusions could I
 7 draw about the document's availability on
 8 the P2P network?

9 MR. SHERMAN: Objection; calls
 10 for speculation. You may answer.

11 A. You couldn't conclude anything
 12 because moments later it could be
 13 available.

14 Q. And in 2008, was it also true
 15 that a document could reside on a distant
 16 node that my search would not reach?

17 A. Yes.

18 Q. When an individual runs a search
 19 on a P2P network and the search identifies
 20 a file, could that file have been found if
 21 the computer on which the file was located
 22 had not been running a file-sharing
 23 application?

24 A. No.

25 Q. I'd like to return your

104

1 Johnson
 2 appears on page 13, the paper states that,
 3 "For a medical testing laboratory, we found
 4 a 1,718-page document containing patient
 5 Social Security numbers, insurance
 6 information and treatment codes for
 7 thousands of patients." Do you see that
 8 text?

9 A. Yes.

10 Q. And did I read it correctly?

11 A. Yes.

12 Q. Does this refer to a LabMD
 13 document?

14 A. Yes.

15 Q. And is it the document that's
 16 excerpted at Figure 4?

17 A. Yes.

18 Q. The final sentence into that
 19 paragraph reads, "All together, almost
 20 9,000 patient identities were exposed in a
 21 single file, easily downloaded from a P2P
 22 network." Do you see that text?

23 A. Yes.

24 Q. And did I read it correctly?

25 A. Yes.

1 Johnson

2 Q. What did you mean by "easily
3 downloaded"?

4 A. That a user who came upon this
5 file could, with a click of the mouse,
6 download the file.

7 Q. Later in the paper, at page 14,
8 you describe the LabMD file and other data
9 identified using your research methodology
10 as having been found -- excuse me, this
11 appears on page 17. If I may direct your
12 attention to page 17, Dean Johnson.

13 A. Yes.

14 Q. You explain at page 17 in the
15 final sentence in the second paragraph
16 that, "...these files were found without
17 extraordinary effort and certainly far less
18 effort than criminals might be economically
19 incited to undertake." Do you see that
20 text?

21 A. Yes.

22 Q. Did I read it correctly?

23 A. Yes.

24 Q. What did you mean by that?

25 A. I meant that those files were in

1 Johnson

2 A. As evident from Figure 8, many of
3 them are just common medical terms, some of
4 which we used in our own digital footprint.

5 Q. But Figure 8 represents search
6 terms that users as opposed to researchers
7 were using on the peer-to-peer network. Is
8 that correct?

9 A. That's correct.

10 Q. And in the right-most column
11 appears, about a third of the way down, the
12 term "lytec medical billing." Are you
13 familiar with Lytec?

14 A. No.

15 Q. Do you know whether Lytec is a
16 type of billing software?

17 A. I don't know.

18 Q. Do you know whether it was used
19 by LabMD?

20 A. I don't know that.

21 Q. Do you know whether it was used
22 to generate the 1,718-page file that's
23 excerpted in Figure 4 of the document that
24 appears in CX382?

25 A. I don't know that.

1 Johnson

2 fact available on a P2P file sharing
3 network, that they could be discovered by
4 anyone looking for them, and that those who
5 are financially motivated to find them
6 would and could invest far more in looking
7 for them than we had.

8 Q. I direct your attention to
9 page 18 of the document that's been marked
10 as CX382. And in Figure 8 you catalog the
11 user-issued searches that you discovered in
12 your research. What is a user-issued
13 search?

14 A. So this is a search term that was
15 typed in by a peer-to-peer file sharing
16 user and observed by Tiversa.

17 Q. So earlier today counsel for
18 LabMD asked you questions about the search
19 terms that you used in identifying files.
20 How do the search terms that appear in
21 Figure 8 at page 18 of CX382 compare with
22 the search terms that you used in Phase 1
23 of the study?

24 MR. SHERMAN: Objection;
25 mischaracterizes the testimony.

1 Johnson

2 Q. I'd like to talk for a moment
3 about the consequences of the inadvertent
4 disclosure of consumer-sensitive personal
5 information.

6 Are there consequences associated
7 with inadvertent disclosure of
8 consumer-sensitive personal information?

9 A. Yes.

10 Q. What are they?

11 A. Consumers can fall victim to
12 various forms of identity theft, including
13 financial identity theft, and in this case,
14 medical identity theft.

15 Q. Let's start with identity theft.
16 What is identity theft?

17 A. The use of personal information
18 to allow a malicious individual to open
19 bank accounts, make financial charges,
20 other forms of fraud.

21 Q. What costs to an individual
22 consumer are associated with identity
23 theft?

24 A. The costs range dramatically from
25 the inconvenience of having your credit

1 Johnson
 2 card cancelled to real financial loss in
 3 cases where loans or other financial
 4 attacks are placed against the individual.
 5 Q. You describe medical identity
 6 theft.
 7 What is medical identity theft?
 8 A. The use of a person's identity to
 9 commit medical fraud.
 10 There are many different cases or
 11 types of medical identity theft. Sometimes
 12 it could be as simple as masquerading as
 13 the person's identity to obtain medical
 14 treatment. In other cases, medical
 15 identity theft can allow individuals to
 16 commit financial fraud against payers,
 17 hospitals.
 18 Q. Are there consequences for
 19 individual consumers that stem from medical
 20 identity theft?
 21 A. The consequences can be more
 22 challenging than even financial theft.
 23 Q. Why is that?
 24 A. Because it's very hard to correct
 25 the problem. Unlike financial, or a

1 Johnson
 2 financial system, where a credit card can
 3 quickly be cancelled, in health care, if
 4 someone is using your identity to receive
 5 treatment, their own medical record becomes
 6 commingled with yours. That can lead to
 7 medical errors in the future or to
 8 misdiagnoses. It also can lead to a long
 9 string of financial obligations that payers
 10 will then track an individual to try to
 11 have them pay for treatment they never
 12 received.
 13 MR. O'LEARY: Can we just go off
 14 the record for just a minute?
 15 MS. RIPOSO VAN DRUFF: Certainly.
 16 (Off the record)
 17 Q. So I'd like to direct your
 18 attention to page 8 of the document that
 19 appears at CX382, the "Data Hemorrhaging"
 20 paper.
 21 And I direct your attention to
 22 the second full paragraph. The third
 23 sentence you describe that, "PHI" -- and
 24 there I believe you're referring to
 25 personal health information -- quote, "can

1 Johnson
 2 be sold and resold before theft occurs."
 3 Do you see that text?
 4 A. Yes.
 5 Q. Did I read it correctly?
 6 A. Maybe I'm not in the right place.
 7 I'm looking at PHI, but I'm not...
 8 MR. O'LEARY: It's here
 9 (indicating).
 10 A. Oh, here. Yup. Okay, I see it.
 11 I'm sorry.
 12 Q. No, that's fine.
 13 And I mischaracterized, I think,
 14 what PHI stands for. In that sentence I
 15 believe that PHI, which is defined on
 16 page 4 of CX382, refers to "protected
 17 health information." Is that correct?
 18 A. Correct.
 19 Q. And on page 8 you say that, "PHI
 20 can be sold and resold before theft
 21 occurs." Is that correct?
 22 A. Correct.
 23 Q. What does that mean?
 24 A. That the value of PHI enables
 25 criminals to sell it multiple times to

1 Johnson
 2 multiple individuals.
 3 Q. And so in the immediate aftermath
 4 of an inadvertent disclosure of an
 5 individual's protected health information,
 6 if medical identity theft has not occurred
 7 in the immediate aftermath, does that mean
 8 that it will not occur?
 9 A. No.
 10 Q. And why not?
 11 A. Because that information has a
 12 long life, a much longer life than a Visa
 13 card number.
 14 Q. Directing your attention to
 15 page ten of CX382, the second full
 16 paragraph begins, "Ironically, individuals
 17 who experience identify theft often never
 18 realize how their data was stolen." Do you
 19 see that text?
 20 A. Yes.
 21 Q. What are you referring to there?
 22 A. We're referring to case examples
 23 where individuals had experienced identity
 24 theft and they themselves often didn't
 25 realize how or why that had occurred.

113

1 Johnson
 2 Q. And why couldn't they track it
 3 back to a specific incident?
 4 A. "They" being the patients?
 5 Q. Yes.
 6 A. Because, again, in this case,
 7 unlike a credit card, where you might know
 8 where you've used it, the PHI often moves
 9 between different providers in the health
 10 care system without their knowledge.
 11 Q. So that's the movement of a
 12 patient's data. But with respect to an
 13 individual who has experienced identity
 14 theft, why is it that they don't realize
 15 how their data was stolen, as described in
 16 your paper at page 10?
 17 A. Well, given that they may not
 18 even be aware of who in the health care
 19 network even had their data, their ability
 20 to know where it was stolen from or how it
 21 was disclosed is exceedingly limited.
 22 Q. Is there anything else that
 23 complicates an individual consumer's
 24 ability to track back the source of
 25 identity theft?

114

1 Johnson
 2 A. In particular, medical identity
 3 theft?
 4 Q. Let's focus on medical identity
 5 theft, yes.
 6 A. Well, in particular, for medical
 7 identity theft, because unlike in the
 8 financial the system where there are credit
 9 monitoring services and credit scores and
 10 widespread sharing of financial activity
 11 and credit worthiness, very little to none
 12 of that exists in the health care sector.
 13 Q. Earlier this morning counsel for
 14 LabMD asked you questions about eliminating
 15 duplicates. This references text that
 16 appears on page 11. Do you remember that
 17 testimony?
 18 A. Yes.
 19 Q. And I refer your attention to the
 20 paragraph that appears below Figure 2. I
 21 believe that you were asked, and I'm
 22 paraphrasing, how you eliminated
 23 duplicates. And my question is: The text
 24 of your paper on page 11 refers to a hash.
 25 What is a hash?

115

1 Johnson
 2 A. A hash is a unique identifier of
 3 a file based on its size and contents.
 4 Q. And if I were to change a single
 5 character in a file, say, add a space
 6 between two words, would the hash of the
 7 original file and the hash of the edited
 8 file be identical?
 9 A. No, they would change.
 10 Q. Did you evaluate the hashes of
 11 documents in order to eliminate duplicates,
 12 as you've described on page 11 of the
 13 document that's been marked as CX382?
 14 A. Yes, though in many cases we also
 15 did this through manual evaluation.
 16 Q. If someone were to search for a
 17 specific document on a P2P network, would
 18 it help to have that document's hash?
 19 A. I'm not sure.
 20 MS. RIPOSO VAN DRUFF: I'd like
 21 to just take a 10-minute break, if we
 22 may, and then I think we can wrap up
 23 quickly.
 24 THE WITNESS: Sure.
 25 (Recess)

116

1 Johnson
 2 EXAMINATION CONTINUED
 3 BY MS. RIPOSO VAN DRUFF:
 4 Q. Earlier today, on counsel for
 5 LabMD's examination, you distinguished
 6 between inadvertent disclosures and
 7 intrusions by an active hacker. Do you
 8 remember that testimony?
 9 A. Yes.
 10 Q. And I believe it was your
 11 testimony -- correct me if I'm mistaken --
 12 that inadvertent disclosures can be
 13 controlled and managed. What did you mean
 14 by that?
 15 A. Well, as we discussed this
 16 morning, the access to information is a key
 17 piece of inadvertent disclosures, and so
 18 limiting access to individuals, and not
 19 just the access, but also their ability to
 20 copy the information or move the
 21 information around.
 22 Q. Are there other things that a
 23 company can do to control or manage
 24 inadvertent disclosures of consumers'
 25 sensitive personal information?

1 Johnson

2 A. There are many, many things far
3 beyond our work, but efforts to eliminate
4 the use of peer-to-peer file sharing within
5 the organization is a start.

6 But things like encryption,
7 encrypting all sensitive information, so
8 that even if it was inadvertently shared it
9 wouldn't be lost or exposed; disabling
10 technologies on laptops or phones that
11 allow the transfer of information, so
12 removing ports on a laptop, for example,
13 segregating information on a computer,
14 personal and private, or, more
15 specifically, sensitive information and
16 nonsensitive information.

17 So there are. There are many.

18 Q. Counsel for LabMD asked you a
19 number of questions and showed you
20 documents relating to your communications
21 with Tiversa, and in particular, with
22 Mr. Gormley. Is that correct?

23 A. Correct.

24 Q. And earlier this morning you
25 didn't remember Mr. Gormley's last name,

1 Johnson

2 Tiversa's technology, that it "monitors
3 global P2P file sharing networks," and you
4 pointed out that the plural was
5 intentional.

6 A. Yes.

7 Q. What did you mean by that?

8 A. That there are several popular
9 networks. Gnutella, which we mentioned
10 earlier is just one of them, but FastTrack
11 is another. EMule is a third. And then
12 there are many more recent ones that keep
13 growing on the Internet.

14 Q. And so, in the first sentence of
15 Footnote 1 in the document that has been
16 marked as Document CX382, when you say that
17 Tiversa "monitors global P2P file-sharing
18 networks," plural, what did you mean?

19 A. I meant that they are actively
20 monitoring many different networks. And in
21 particular, why that's relevant for me and
22 my research, is that it allows -- the
23 collaboration with them allows us to look
24 at many networks. Individual users might
25 only participate in one, but there are many

1 Johnson

2 correct?

3 A. Yes.

4 Q. But you characterized him, in
5 what I think was a joke, as a friend of
6 yours. Is that correct?

7 A. Introduced by a mutual friend.

8 Q. So Mr. Gormley is not a friend of
9 yours --

10 A. That's correct.

11 Q. -- is that right?

12 A. That's correct.

13 Q. In fact, he's a research
14 associate of yours?

15 A. That's correct.

16 Q. I'm going to follow up on
17 something that you said in response to a
18 question from counsel of LabMD about
19 Footnote 1 in documents that counsel for
20 LabMD marked as RX-3 but that I've also
21 marked as CX382. And I would ask you to
22 take a look at Footnote 1.

23 A. Yes.

24 Q. You made a point to note that, in
25 the first sentence, where you described

1 Johnson

2 different networks.

3 Q. And so, for example, Tiversa's
4 technology is not limited to users who are
5 using the LimeWire client, is it?

6 A. That's correct, it's not.

7 LimeWire operates on the Gnutella network.

8 There are other clients that operate on
9 Gnutella, but there's yet a whole other set

10 of clients that operate on eMule or

11 FastTrack.

12 Q. Counsel for LabMD asked you about
13 the way that you searched for files in
14 Phase 1 of the research that resulted in
15 CX382. Do you remember that testimony?

16 A. Yes.

17 Q. And I believe it was your
18 testimony, and correct me if I am mistaken,
19 that you were only able to download a file
20 if the user made the file, quote,
21 publically available. Do you remember that
22 testimony?

23 A. Yes.

24 Q. What do you mean by "publicly
25 available"?

1 Johnson

2 A. It means that the file was shared
3 in the directory that was accessed by a
4 file-sharing client that they had resident
5 on their computer.

6 Q. And absent a file-sharing client,
7 would there be a way to access that file?

8 A. No.

9 Q. Counsel for LabMD also asked you
10 about your impression of the level of
11 awareness of the risks opposed by P2P
12 file-sharing applications.

13 Do you remember that testimony?

14 A. Yes.

15 Q. In describing the awareness of
16 the risks of P2P file-sharing applications
17 in 2008, would you draw a distinction
18 between the awareness of ordinary consumers
19 and the awareness of information security
20 professionals?

21 A. I think even further, I think
22 there was awareness within the research
23 community. I think even among computer
24 security professionals during that time, I
25 would say that there was awareness, but not

1 Johnson

2 as deep as you might believe. And
3 certainly, among the consumer public, not
4 deep at all.

5 Q. Well, let's set aside the
6 consumer public. But security
7 professionals were aware of the risks posed
8 by P2P file-sharing applications, correct?

9 A. They were, though I think that
10 many may not have realized how pervasively
11 they were being used within organizations.

12 Q. How could a security professional
13 have evaluated whether a peer-to-peer
14 file-sharing application was used within
15 his or her organization?

16 MR. SHERMAN: Objection; calls
17 for speculation. You may answer.

18 A. There are several different
19 approaches. One would be to look for large
20 amounts of traffic going to and from a
21 particular computer within their network.
22 Direct inspection of the computers
23 themselves, that is, inspecting the
24 applications that were running on that
25 computer, could be another approach.

1 Johnson

2 Q. This morning in a response to
3 counsel for LabMD you described the browse
4 host function in LimeWire. Do you remember
5 that testimony?

6 A. Yes.

7 Q. If a user were using LimeWire and
8 found a file that he or she wanted, what
9 would the browse host function allow that
10 user to then do?

11 A. It would allow the user to see
12 other files the same user was sharing.

13 Q. So would it allow the user who
14 had conducted the search to view all other
15 files that the user on whose computer the
16 search had located a file was making
17 publicly available?

18 A. Yes.

19 Q. And could that user then download
20 any files that he or she chose?

21 A. Yes.

22 Q. Okay. I'd like to return your
23 attention, please, to RX-9, which is
24 probably in this pile here.

25 A. Oh, got you. Yes.

1 Johnson

2 Q. Okay. So RX-9, counsel for LabMD
3 asked you a number of questions about pages
4 2 -- well, about page 2 of the document.
5 Page 1 of the document is -- well, can you
6 describe page 1 of the document that
7 appears at RX-9?

8 A. Are we looking at the same...

9 Q. No, I'm asking for the very first
10 page that appears on RX-9.

11 A. It appears to be the bottom an
12 e-mail from another document.

13 Q. And so, does page 1 of RX-9 bear
14 any relationship to pages 2, 3, and 4 of
15 RX-9?

16 A. No.

17 Q. So just to be clear, page 1 of
18 RX-9 includes the e-mail signature block of
19 Mr. Settlemyer, an attorney at the Federal
20 Trade Commission. Is that right?

21 A. That's right. And it's also
22 listed in the upper right-hand corner as
23 Eric Johnson - 000023. And I'm just here
24 referencing page 1, but I think we've been
25 referencing these numbers.

1 Johnson
 2 Q. Terrific. Yes, that's a very
 3 helpful clarification. Thank you, Dean
 4 Johnson.
 5 Did Mr. Settlemyer have anything
 6 to do with the confidentiality agreement
 7 between you and Tiversa?
 8 A. No.
 9 Q. Counsel for LabMD asked you about
 10 the process by which you evaluated
 11 Tiversa's technology --
 12 A. Yes.
 13 Q. -- do you remember that
 14 testimony?
 15 A. Yes.
 16 Q. Did you draw any conclusions
 17 about Tiversa's technology?
 18 A. Yes. We concluded that they had
 19 substantial capabilities to locate and
 20 observe files on peer-to-peer file sharing
 21 networks.
 22 Q. And that's the reason that you
 23 partnered with them in your research?
 24 A. Yes.
 25 MS. RIPOSO VAN DRAFF: Subject to

1 Johnson
 2 any limited redirect, I'm happy to
 3 tender.
 4 MR. SHERMAN: Okay. I have a
 5 couple of questions. And we don't have
 6 to switch, because I'm going to be very
 7 quick.
 8 MS. RIPOSO VAN DRUFF: Okay.
 9 MR. SHERMAN: I think.
 10 RE-EXAMINATION
 11 BY MR. SHERMAN:
 12 Q. So you just said that Tiversa had
 13 substantial capabilities to locate files,
 14 correct?
 15 A. Yes.
 16 Q. And that's why you partnered with
 17 them in your research of file sharing on
 18 peer-to-peer networks?
 19 A. Yes.
 20 Q. You, moments ago, however,
 21 testified that on page 17 of the hemorrhage
 22 study -- and I don't care which one you
 23 use --
 24 A. Yup. Okay.
 25 Q. -- it was pointed out by

1 Johnson
 2 complaint counsel that the statement in
 3 there says, "It is important to note that
 4 all of these files were found without
 5 extraordinary effort and certainly far less
 6 effort than criminals might be economically
 7 incited to undertake."
 8 And you said, yes, they could be
 9 found by anyone looking for them.
 10 A. Yes.
 11 Q. Yet you used Tiversa's
 12 substantial capabilities to find the files?
 13 A. Yes.
 14 Q. And, in fact, you've described
 15 circumstances under which files could not
 16 be found by anyone looking for them for the
 17 mere reason that the file may be located
 18 too many hosts away for them to actually
 19 find the file, correct?
 20 A. For an individual user, yes.
 21 Q. For an individual user.
 22 And are we then assuming that
 23 criminals may not be individual users; they
 24 may be some vast organization with the
 25 capabilities of Tiversa?

1 Johnson
 2 A. We believe some are.
 3 Q. Some are.
 4 But the file just isn't available
 5 to anyone looking for them, then, is it?
 6 A. They have to have the same
 7 client -- operate on the same network,
 8 excuse me. And certainly, if my computer
 9 is not turned on, or if I'm not sharing,
 10 they're not going to be able to see it.
 11 Q. So there are a variety of
 12 factors, including the technology that they
 13 might be using, that would determine
 14 whether or not they would be able to find
 15 the file that they're looking for, correct?
 16 A. Yes.
 17 Q. Are there any security measures
 18 in place for the documentation that was
 19 captured and utilized in the "Hemorrhaging"
 20 study by Dartmouth?
 21 A. Yes.
 22 MS. RIPOSO VAN DRUFF: Objection;
 23 vague as to "security measures."
 24 Q. So those documents are protected
 25 from third-party access?

1 Johnson
 2 A. Yes.
 3 Q. In what manner?
 4 A. They're, first of all, not on a
 5 computer that's on the Internet; secondly,
 6 they are in encrypted password-protected
 7 files; third, they are stored in secured
 8 rooms.
 9 MR. SHERMAN: I have nothing
 10 further.
 11 MS. RIPOSO VAN DRUFF: Nor do I.
 12 MR. O'LEARY: So, just before we
 13 go off the record, since there's a
 14 nondisclosure agreement between Eric
 15 and Tiversa, we would like to have RX-9
 16 and 10 and 4 and 5 and 7 marked as
 17 confidential.
 18 MS. RIPOSO VAN DRUFF: We have no
 19 objection.
 20 MR. O'LEARY: Hopefully that
 21 doesn't interfere with your ability to
 22 use them.
 23 And the witness will read and
 24 sign, please.
 25 (Time noted: 2:00 p.m.)

1 Johnson
 2
 3
 4
 5
 6
 7 M. ERIC JOHNSON, Ph.D.
 8
 9 Subscribed and sworn to
 10 before me this day
 11 of 2014
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25

1 Johnson
 2 February 18, 2014
 3
 4 ERRATA
 5
 6 PAGE/LINE CHANGE/REASON
 7 _____
 8 _____
 9 _____
 10 _____
 11 _____
 12 _____
 13 _____
 14 _____
 15 _____
 16 _____
 17 _____
 18 _____
 19 _____
 20 _____
 21 _____
 22 _____
 23 _____
 24 _____
 25 _____

1
 2 CERTIFICATE
 3
 4 STATE OF NEW YORK)
 5) ss.
 6 COUNTY OF NEW YORK)
 7
 8 I, Alexis Perez Jenio, a Shorthand
 9 Reporter and Notary Public within and for
 10 the State of New York, do hereby certify:
 11 That M. ERIC JOHNSON, Ph.D., the
 12 witness whose deposition is hereinbefore set
 13 forth, was duly sworn by me and that such
 14 deposition is a true record of the testimony
 15 given by such witness.
 16 I further certify that I am not
 17 related to any of the parties to this action
 18 by blood or marriage and that I am in no way
 19 interested in the outcome of this matter.
 20
 21
 22
 23 ALEXIS PEREZ JENIO
 24
 25

1			
2	February 18, 2014		
3			
	INDEX		
4			
5	WITNESS EXAMINATION BY PAGE		
6	M. Eric Johnson Mr. Sherman 3, 126		
	Ms. Riposo Van Druff 92		
7			
8	EXHIBIT		
9	RX PAGE		
10	1 4	One-page cover letter with	
		attached Subpoena ad	
11		Testificandum	
12	2 10	Homeland Security Grant	
		Award Terms and Conditions	
13			
14	3 16	Article titled "Data	
		Hemorrhage on the	
15		Healthcare Sector," Bates	
		stamped Eric Johnson -	
16		000003 through 24	
17	4 41	Four-page e-mail string	
18	5 44	Two-page e-mail string	
19	6 45	Four-page spreadsheet,	
		first page being blank	
20	7 61	Three-page e-mail chain	
21	8 67	Six-page double-sided	
		E-mail string, Bates	
22		stamped Eric Johnson -	
		000001 and 2, 21 and 22,	
23		and 27 through 34	
24			
25			

1			
2	February 18, 2014		
3			
	INDEX (Continued)		
4			
5	RX PAGE		
6			
7	9 74	Two-page double sided	
		confidentiality agreement,	
8		Bates stamped Eric Johnson	
		000023 through 26	
9	10 78	Two-page e-mail string	
10	11 83	Four-page excerpt from	
		"Information Governance;	
11		Flexibility and Control	
		Through Escalation and	
12		Incentives," dated	
		April 24, 2008	
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

A				
ability 55:5 56:25 113:19,24 116:19 129:21	agreeable 27:24	121:16 122:8,24	attended 19:12	Bates 16:4 67:15,24 74:21 99:9 103:5 103:24 133:14,21 134:7
able 28:15 31:7,18 32:11 48:3,6 50:12 76:25 99:18 120:19 128:10,14	Agreed 8:17	applied 86:7,8	attention 99:6 103:2 103:23 105:12 106:8 110:18,21 112:14 114:19 123:23	bear 124:13
absent 121:6	agreement 11:10 74:21 75:10,11 125:6 129:14 134:7	applying 88:20	attorney 92:14 124:19	BearShare 35:9
academia 9:17	Alain 2:19 92:17	appreciate 55:15	Attorneys 2:6	began 60:20
academic 82:14 96:18	Alexis 1:18 132:8,23	appreciated 70:5	author 15:6	begins 112:16
acceptable 85:24	allow 29:10 30:21 31:22 38:3 81:10 108:18 109:15 117:11 123:9,11 123:13	approach 59:13 87:14 122:25	availability 26:22 73:18 101:9 102:7	belief 80:19
access 37:18 38:2 85:8,10,15 86:4,7 86:11,14,23 87:3,5 87:23 88:8,10,15 88:18,23 89:2,4,22 116:16,18,19 121:7 128:25	allowed 49:14 56:14 97:20 98:4	approaches 122:19	available 36:7 48:7 48:8,10 77:14 100:10 102:13 106:2 120:21,25 123:17 128:4	believe 10:21 11:3,5 11:24 12:16 24:9 28:12 37:9 48:9 50:11 55:13 69:11 72:16 75:15 79:16 90:12,24 103:14 110:24 111:15 114:21 116:10 120:17 122:2 128:2
accessed 121:3	allowing 34:10 80:25	April 62:3,17 65:18 83:19 84:18 134:12	Avenue 2:7,15	believed 39:24 40:22
accounts 100:16 108:19	allows 30:10 97:3 119:22,23	area 9:13 39:11,22 72:25 73:2 95:22 96:3	Award 10:16 133:12	bell 24:15
accurate 10:5 36:2	amendments 11:6	areas 21:18 87:8	awarded 15:12	beneficial 86:14
acknowledgments 20:20 21:12	AMERICA 1:2	argumentative 49:12	aware 15:11 16:24 23:20 39:25 40:4 55:4 56:14 80:24 82:18 83:4,8,9 85:21 113:18 122:7	benefit 93:2,17
action 132:17	amounts 122:20	article 10:9 15:2,4,7 15:13,21 16:2,3,8 16:9,13,19 17:7,13 17:21,25 18:12,20 20:15,17 21:22 22:25 24:22 26:10 37:3,5 40:10 49:8 68:25,25 69:2 72:8 81:23 133:13	awaresness 39:15,23 121:11,15,18,19 121:22,25	better 89:23 91:4
active 90:23 116:7	analysis 21:19 27:15 40:11,14 46:11 53:11	articles 22:4 51:5 96:9,14	a.m. 1:9	beyond 85:17 117:3
actively 119:19	and/or 26:16	articulate 30:9 31:6		big 62:8
activities 37:19	answer 7:17,17 50:21 54:15,23 58:19 71:18 100:4 101:12 102:10 122:17	aside 122:5	B	billing 107:12,16
activity 31:19,21 40:24 114:10	answered 70:12	asked 20:23 66:25 70:12 106:18 114:14,21 117:18 120:12 121:9 124:3 125:9	B 56:5	blank 45:12 133:19
ad 4:23 133:10	anyway 5:17	asking 7:14,16,18 13:6,25 14:4,21 30:17,18,20 51:23 124:9	Bachelor 6:7,9	blind 20:7
add 115:5	anyways 11:25	asks 34:13	back 6:22 8:21 12:21 34:16 39:14 43:2 46:9 47:6 50:23 61:22 93:11 113:3,24	block 124:18
added 44:21	apologize 67:2	aspect 27:12	background 6:5 21:18,25 51:24	blood 132:18
additional 45:3	appear 29:17,20 106:20	assistant 47:18	backwards 61:18	blow 100:11,12
address 49:25 50:4	APPEARANCES 2:2 3:2	assisted 81:25	bank 87:12 108:19	blowing 100:10
addresses 49:5,10 49:19 50:5	appeared 57:5,13 58:13	associate 118:14	banking 25:20 40:21 69:13,15 70:14,17 71:12 72:3	board 11:7 82:2
ADMINISTRATI... 1:3	appears 32:20 41:23 41:25 42:25 75:9 78:16 79:19 84:3 84:20 88:5 93:4,20 93:22 95:14,19 99:9 103:7 104:2 105:11 107:11,24 110:19 114:16,20 124:7,10,11	associated 11:18 12:17 13:10 45:24 51:5 53:19,22 108:6,22	based 27:23 29:17 39:11 50:2 63:24 66:16 85:15 88:10 115:3	boards 98:23
advantage 31:18	application 51:22 102:23 122:14	assume 65:9	basically 8:6,22 9:16 72:23	boost 63:17 65:8
advised 5:4	applications 121:12	assuming 127:22		bottom 47:4 78:17 124:11
affect 100:17		attached 4:23 5:14 5:20,21,25 133:10		brands 43:19
affiliated 8:22 43:18 57:16,22,24		attacks 109:4		breaches 23:17,18 23:19 25:25
aftermath 112:3,7				break 7:23,24 8:3 41:10,19 74:17 89:7 115:21
afternoon 92:11				briefly 73:21
agency 66:2 95:2,6				broad 40:23 57:25 90:21
aging 103:9				broader 53:24 97:17 98:4,6
ago 8:24 9:2 126:20				broadly 52:6
agree 5:25 16:10,11 28:24 38:13 52:22				browse 57:3,8 58:11 59:21,25 60:4

123:3,9	109:3,10,14	click 105:5	71:21	consist 76:22
browser 67:3	115:14	client 32:2,8 120:5	complicates 113:23	consistent 57:15
building 74:2	cast 58:2	121:4,6 128:7	compound 26:19	consortium 17:3,6,9
bump 24:2	catalog 106:10	clients 56:24 120:8	comprising 48:13	17:16,24
BUREAU 2:14	category 52:16	120:10	computer 29:22	constantly 34:20
business 6:17 9:8	Center 6:18	clinics 43:19	33:15 35:25 37:15	67:7 100:25
34:9 77:9 86:8	certain 10:5 69:19	codes 59:17 104:6	49:24 55:13	consult 8:5
	70:24 78:3 79:18	coined 100:8	102:21 117:13	consumer 2:14
	certainly 55:23	collaboration 11:14	121:5,23 122:21	98:19 108:22
C	63:18 83:14 89:9	11:19 28:7 119:23	122:25 123:15	122:3,6
C 56:5	91:19 105:17	colleague 92:17	128:8 129:5	consumers 96:11
calendar 12:22 13:4	110:15 122:3	collect 37:8 40:14	computers 29:23	108:11 109:19
call 19:16 22:14	127:5 128:8	collected 37:7,10,12	31:11,15 33:23,24	116:24 121:18
23:19,25 62:12	CERTIFICATE	collection 37:19	122:22	consumer's 113:23
74:5 91:6,11	132:2	66:2 79:13	computer-driven	consumer-sensitive
called 4:3 18:4 20:7	certify 132:10,16	college 3:5 6:6,16	9:25	108:4,8
57:2	cetera 43:19	8:23 9:9 10:3 11:7	concept 100:8	contact 12:2,5 23:15
calls 12:6 85:24	chain 61:13 133:20	17:21	concepts 88:9	contained 51:20
90:19 91:9,17	challenge 91:21	column 107:10	concerning 25:24	containing 53:21
101:11 102:9	challenges 68:18	come 22:9 23:14	26:11	59:16 104:4
122:16	challenging 97:16	50:23	conclude 101:13	contains 78:17
cancelled 109:2	109:22	comfortable 14:9	102:11	contents 45:19
110:3	chance 63:13	coming 62:8 63:2	concluded 125:18	99:17 115:3
capabilities 40:5	change 87:16 115:4	commingled 110:6	conclusions 101:8	context 62:18
125:19 126:13	115:9	Commission 1:2	102:6 125:16	continued 3:2 41:14
127:12,25	CHANGE/REAS...	2:13 92:14 95:11	Conditions 10:17	60:21 74:25 83:13
capacity 9:7,20	130:6	95:16 124:20	133:12	89:12 116:2 134:3
capture 31:18,20	changing 34:20 67:7	commit 71:13 109:9	conduct 17:5 21:17	contract 10:3,8
53:25	101:4,5	109:16	98:15	12:16 52:15
captured 47:6,23,25	character 115:5	committee 69:16	conducted 12:25	contracting 34:21
48:5,8,9 50:18	characterize 13:9	82:5	17:18,20,21 19:24	67:9
58:7 59:23 60:3	31:3 58:10	common 47:3 51:3	20:2 22:6,8 25:3,5	contracts 11:6 12:8
63:9 66:21 80:20	characterized 118:4	107:3	28:7 60:17 76:23	13:10
128:19	charges 108:19	communicate 55:25	94:22 123:14	contribute 95:12
card 62:13 109:2	chart 42:18,21	communicated 56:6	conducting 81:16	96:2,5
110:2 112:13	check 83:14 85:3	communication	Conference 94:2	control 83:18 84:15
113:7	choose 82:16	82:21,23	conferences 96:18	116:23 134:11
care 10:10 25:12,20	choosing 20:12	communications	confidential 76:4	controlled 90:25
26:12 27:7 40:25	chose 97:18 123:20	63:25 65:10	129:17	116:13
42:2 43:4,6,23	Chris 24:9 41:24	117:20	confidentiality	controls 89:24
46:7,16,25 47:13	44:10 61:24 79:4	communities 33:21	74:21 75:9,11	conversation 63:8
53:20 57:17,25	80:9	community 121:23	125:6 134:7	70:19 72:17,19
71:4,7 72:2,4	circumstances	company 116:23	confirm 5:3	conversations 69:22
89:22 110:3	86:19 101:21	compare 106:21	Congress 96:21	70:9,15 72:23
113:10,18 114:12	127:15	comparing 71:8	connection 75:16	73:17
126:22	claimed 77:2	comparison 42:16	consequences 108:3	conveying 59:9
Carl 68:21 69:5	clarification 15:14	complaint 92:5,15	108:6 109:18,21	coordinate 63:18
73:14	93:16 125:3	127:2	consider 42:15	copies 48:18
case 19:17 21:5 46:4	clean 8:16	complaints 21:23	53:18	copy 5:8,11,18
65:25 88:15	cleaners 97:13	22:7	consideration 41:2	48:21,25 49:7
108:13 112:22	clear 14:22,24 66:17	complete 85:3 88:4	considered 33:25	68:24 88:5 93:4
113:6	124:17	94:3	42:14 46:5 48:17	94:3 99:7 116:20
cases 37:24,25 38:7	clearly 15:20	complex 71:4,7,19	52:2	copying 99:11
38:8 39:3 49:22				

core 29:9	create 39:9,23	99:7 103:3 105:8	describes 99:11	disclosed 97:10,22
corner 124:22	created 77:11 78:2	110:19 112:18	describing 86:3 88:8	97:25 113:21
corporation 1:6	95:4 96:10	113:12,15,19	121:15	disclosure 90:23
corporations 96:9	creating 21:20	133:13	description 34:17	96:11 97:5 98:7
correct 4:10 8:23	53:20 74:13	database 63:16 65:7	designed 98:18	108:4,7 112:4
9:5 11:23 15:4,7	creation 74:7	65:11,17	detailed 51:23	disclosures 25:4
16:16 19:4 21:13	credit 108:25 110:2	databases 65:17	details 37:10	38:13,16 89:20
21:14 22:20 27:13	113:7 114:8,9,11	date 60:11 84:19	detect 89:25	90:25 97:15,19
28:5 32:20,22,23	criminal 25:6 26:8	dated 44:11 68:21	determination	116:6,12,17,24
36:12,13 44:12	criminals 105:18	70:4 72:6 73:15	47:14 48:4	discover 76:25
48:18,19 49:13,20	111:25 127:6,23	78:22 80:13 83:19	determine 50:17	discovered 51:19
51:12 56:17,18	cross 40:24	134:12	52:24 53:6 76:24	58:15 106:3,11
62:3 65:9 66:7	Crypto 93:25	dates 12:22 13:5,7	85:4 128:13	discuss 72:9 90:22
68:22 69:2 71:10	current 82:23	85:4	determined 57:8	discussed 48:12
75:12 78:20 80:11	customarily 19:17	DAUGHERTY 3:12	67:2	64:10 74:5 75:17
84:16 86:24,25	customer 95:8	Daughterty 94:11	develop 43:14 96:23	116:15
87:6 90:2 107:8,9	customers 94:20	day 100:22,22	98:12	discussion 16:13
109:24 111:17,18	CX0382 93:3	131:10	developed 28:8	74:8
111:21,22 116:11	CX382 93:20 94:7	DC 2:9,17	33:20 43:5 98:14	discussions 12:7
117:22,23 118:2,6	94:14 95:14,19	dean 9:8 79:2 92:11	developing 9:22	72:14
118:10,12,15	99:7 103:3 106:10	93:17 95:22	96:6	distant 101:24,25
120:6,18 122:8	106:21 107:24	105:12 125:3	development 9:21	102:15
126:14 127:19	110:19 111:16	December 73:15	difference 29:25	distinct 31:17
128:15	112:15 115:13	decided 46:6	31:6 90:21	distinction 34:6
correctly 28:11	118:21 119:16	deep 122:2,4	differences 30:8	121:17
35:14 46:19 51:8	120:15	define 12:5 13:16	different 17:18,19	distinguish 50:6
52:17 53:16 57:6	cyber 11:13,19	17:8 48:20 85:9	23:17 25:19 28:22	distinguished 116:5
59:19 62:14 63:22	14:20	defined 54:16	29:3,5 30:22 33:3	distributed 77:12
87:17 104:10,24		111:15	33:19 37:20 46:25	disturbing 52:11
105:22 111:5		definition 14:12	50:3,4,5,10,13	59:14
costs 108:21,24	D	49:8	56:16 67:11 72:2	DOCKET 1:5
counsel 3:6 5:7 8:5	D 3:9	deliberate 68:2,3,9	97:9 100:16	document 6:2 10:22
67:23 76:10 78:25	dangerous 51:11,19	Department 10:4	109:10 113:9	10:24 11:5,10
92:3,5,16 106:17	52:2,3,19 58:25	11:8 12:3,10 14:18	119:20 120:2	17:17 41:17 51:22
114:13 116:4	dangers 39:17 74:4	16:14 18:9 19:3,10	122:18	52:20,25 59:15
117:18 118:18,19	Dartmouth 3:5 6:16	19:15,25 20:4,10	differently 29:10	73:7 92:6 93:3,7
120:12 121:9	8:23 9:9 10:3 11:7	depending 33:16	digital 6:19,20 32:15	93:19,22 99:6
123:3 124:2 125:9	11:18 17:21 20:16	depends 51:13	43:6,10 44:21	101:7 102:5,15
127:2	20:24 21:4 37:15	86:18	46:13,21,22,24	103:2,13,15 104:4
country 77:13	37:17,17 47:21	deposition 1:14 7:3	47:8 53:20,21	104:13,15 106:9
COUNTY 132:6	48:7 53:4 54:12,18	75:18 132:12,14	63:21 64:22 65:2	107:23 110:18
couple 63:13 83:15	54:20 55:2 77:4	describe 11:17	100:8,12 107:4	115:13,17 119:15
89:14 126:5	79:11 80:25 82:3,8	38:10 56:20 77:24	DINSMORE 2:5	119:16 124:4,5,6
Coupled 89:19	83:6 128:20	87:7 97:8 100:2	direct 99:5 103:23	124:12
coupling 89:21	data 10:9 15:2 16:3	105:8 109:5	105:11 106:8	documentation
course 18:15 47:7	17:7,12,20,24	110:23 124:6	110:17,21 122:22	128:18
court 7:8,19 8:8,15	18:11,20 20:14	described 28:6 30:2	directed 79:2,4 95:3	documents 11:23
10:14	21:19 22:24 24:22	43:11 50:14 53:7	Directing 112:14	51:5,11,19 53:7
cover 4:22 68:16	25:24,25 26:10	55:5 56:22 57:11	director 6:18	73:3 80:20 94:15
133:10	32:16 37:2 40:15	60:10 71:18 98:8	directory 121:3	94:24 95:3 115:11
co-author 84:9	41:5 58:25 68:4,25	113:15 115:12	disabling 117:9	117:20 118:19
co-contributor	71:10,11,12,12,15	118:25 123:3	discernible 66:22	128:24
84:10	71:19,24 80:22	127:14	disclose 62:10 76:4	document's 101:9
	89:16,19 93:25			

102:7 115:18
doing 29:4 39:5,13
 46:5 82:4
dominant 87:15
double 74:20 134:6
double-sided 67:14
 133:21
download 35:25
 105:6 120:19
 123:19
downloaded 35:10
 35:17 104:21
 105:3
Downloading 35:19
Dr 4:7 6:23 22:21
 75:3 83:22
DRAFF 125:25
draft 95:17
dramatically 108:24
draw 101:9 102:7
 121:17 125:16
drive 37:25 88:24
 97:13
driven 34:8
Druft 2:18 5:7,12
 18:5 26:18 27:4
 29:12,19 30:14,23
 31:9,12 39:18 40:7
 41:8 49:11 50:19
 53:2 55:21 56:11
 57:18,21 58:17
 59:7 62:20 67:23
 68:7 70:11 74:18
 76:9 78:24 79:22
 81:12 82:25 85:23
 87:25 88:21 89:9
 90:18 91:7,16,24
 92:10,25 93:15
 110:15 115:20
 116:3 126:8
 128:22 129:11,18
 133:6
duly 4:3 132:13
duplicate 48:17,21
 93:10
duplicates 114:15
 114:23 115:11
DVD 37:24

E

earlier 17:15 23:13
 48:12 50:15 66:4
 98:8 106:17

114:13 116:4
 117:24 119:10
early 75:17,23
easily 35:10,17
 66:22 104:21
 105:2
East 1:17
easy 50:12
economically
 105:18 127:6
economics 6:8
edited 115:7
editorial 98:23
education 6:6
educational 6:5 74:2
 74:7,13
effort 17:16 53:6
 105:17,18 127:5,6
efforts 13:13 117:3
elements 25:6 26:9
 27:9
eliminate 115:11
 117:3
eliminated 114:22
eliminating 114:14
employed 9:10
employee 76:11
 86:21 91:5
employees 52:14
 76:14 79:8 85:14
 86:19 88:11
employer 76:5,11,13
employment 6:14
 9:16 51:23
employs 88:9
EMule 119:11
 120:10
enabled 56:23
enables 111:24
encrypted 129:6
encrypting 117:7
encryption 117:6
engineer 9:21
engineering 6:9,11
 6:12
enhancements
 34:19
entire 32:6
entities 42:8,23
entitled 84:13
envisioning 33:4
equivalent 30:7
Eric 1:14 4:2 16:5

62:6 67:15 74:22
 124:23 129:14
 131:7 132:11
 133:6,15,22 134:7
ERRATA 130:4
error 93:12
errors 110:7
Escalation 83:18
 84:15 134:11
establishments 72:4
et 43:19
evaluate 76:7,16
 115:10
evaluated 122:13
 125:10
evaluating 77:7
evaluation 20:12
 76:18,21 77:9
 115:15
evident 107:2
exact 12:22 13:5,6
 18:17 60:11 93:9
exactly 37:10 54:17
examination 4:5
 41:14 74:25 89:12
 92:9 116:2,5 133:5
examine 56:25
examined 25:11
 26:21 57:4,9 58:12
 58:24
examining 25:3,6
example 27:11
 31:25 37:4 43:18
 77:25 87:12 97:11
 117:12 120:3
examples 50:9 55:24
 56:3,5,8,10 112:22
exceedingly 113:21
exceptions 33:18
excerpt 83:16 84:7
 103:12,14 134:10
excerpted 88:6
 104:16 107:23
exchange 73:3
excuse 67:25 105:10
 128:8
executed 75:14
exhaustive 32:6,12
exhibit 4:13,24
 10:17 16:6 41:13
 44:4 45:12 46:3
 61:14 67:17 74:23
 78:10 83:20 93:6

133:8
exists 114:12
expanding 67:9
experience 112:17
experienced 112:23
 113:13
experiments 28:6
 76:24 98:18,22
expert 85:25 90:20
 91:10,18 98:16
explain 105:14
explicitly 37:9
exploit 99:17
exposed 99:12,14
 104:20 117:9
extent 20:21 25:17
 37:22 76:6,15 88:3
 92:2
extraordinary
 105:17 127:5
e-mail 38:7 41:12,24
 42:6 44:3,9 61:13
 62:23 64:10 65:10
 65:18 67:14 68:21
 70:3 71:2 72:6,17
 73:6,14 78:9,17,25
 124:12,18 133:16
 133:17,20,21
 134:9
e-mails 12:6 61:24
 62:2 64:12 68:15
 69:24

F

faces 99:16
facilitate 51:21
facilities 42:2
fact 9:2 33:16 42:17
 45:5 54:11 56:19
 56:22 71:11 76:24
 97:14 101:4 106:2
 118:13 127:14
factories 96:7
factors 128:12
faculty 82:12,14
failed 34:7
fair 9:15 10:9 13:8
 18:19 23:8 31:3
 39:14 40:2 42:11
 57:14 58:10 59:21
 59:25 60:22 61:23
 64:2,5 87:19 88:17
fall 108:11

false 47:10,11,15
familiar 15:3 107:13
far 8:21 59:14
 105:17 106:6
 117:2 127:5
FastTrack 119:10
 120:11
feature 34:4
features 56:23
February 1:8 68:22
 70:4 94:2 130:2
 133:2 134:2
Federal 1:2 2:13
 25:14 92:14 95:11
 95:16 124:19
feel 7:23 48:22
Figure 48:15 51:18
 65:23 103:7,8,9
 104:16 106:10,21
 107:2,5,23 114:20
file 25:7 26:3,4,5,16
 26:21,22 27:12,15
 28:10,16,18 31:16
 32:3,15,15 34:10
 34:11,15 35:8,20
 35:24 36:4,10,11
 36:15,19,20,22
 37:22 38:9 39:12
 40:4 45:24 47:9,15
 49:4,9,15,18,23
 50:4,10,18 52:7
 60:2,8 66:15,18
 74:4,9 77:25 78:4
 78:5,6,8 79:13
 96:24 97:19,25
 98:2 99:14,16,21
 99:24 100:16,18
 101:19,22 102:20
 102:20,21 104:21
 105:5,6,8 106:2,15
 107:22 115:3,5,7,8
 117:4 119:3
 120:19,20 121:2,7
 123:8,16 125:20
 126:17 127:17,19
 128:4,15
files 27:15 31:23,23
 35:7 37:6,8,10,12
 37:14,16,24 38:3
 38:23 39:8 46:16
 47:6,13,22 48:5,8
 48:9,14,17 51:4,20
 53:25 54:7,13

- 56:25 57:5,13 58:7
58:14,15,24 59:14
62:24 63:3,4,9
64:14,18 66:21
76:25 77:8,11,14
77:16,19 97:21,23
97:24 99:11 100:5
100:9 105:16,25
106:19 120:13
123:12,15,20
125:20 126:13
127:4,12,15 129:7
file-sharing 73:19
77:15 102:22
119:17 121:4,6,12
121:16 122:8,14
final 42:14 104:18
105:15
finalized 95:19
financial 25:5 26:8
27:6 71:9,14,14
81:3 93:25 108:13
108:19 109:2,3,16
109:22,25 110:2,9
114:8,10
financially 106:5
find 25:8 34:11
36:16,17 55:8,12
56:4,10 62:13
77:16,18 78:4
101:8,22 102:6
106:5 127:12,19
128:14
finding 55:24 56:2,7
64:15 95:8
findings 37:22 62:11
finds 63:14
fine 111:12
finish 7:16
finished 63:3 89:8
firm 46:25
firms 40:17 43:5,23
53:20,22 57:17,25
91:20
first 11:9 28:3 35:4
37:5 38:11 39:7,22
41:20 42:11 45:11
47:5 51:2,2 52:10
54:10 55:19 58:4,8
58:16,23 59:3,10
60:5,13,17,23
68:20 78:18 79:14
84:7 85:6 87:11
- 93:12 99:10
118:25 119:14
124:9 129:4
133:19
five-minute 89:7
flash 97:12
Flexibility 83:17
84:14 134:11
focus 40:18 46:7
53:4 66:5 95:23
114:4
focused 26:16 38:12
40:15 72:23
focusing 40:22 41:3
follow 8:14 55:5
118:16
followed 51:5
following 40:20
follows 4:4
Footnote 28:4
118:19,22 119:15
footprint 43:6,10
44:22 46:22 47:9
53:21 107:4
forget 97:13
forgot 63:19
form 11:25 18:17
88:2,6,22
formal 76:18
forms 23:17 108:12
108:20
forth 132:13
Fortune 40:16 42:6
found 27:15 47:10
51:4,11 52:12
58:25 59:15 62:25
63:16 64:20 65:7
65:11,16 74:9
101:18 102:20
104:3 105:10,16
123:8 127:4,9,16
foundation 29:13
30:24 79:23
four 26:7 27:3 48:12
84:7
fourth 45:17
Four-page 41:12
45:11 83:16
133:16,18 134:10
fragmented 71:25
frame 37:13 60:9,10
fraud 71:14 108:20
109:9,16
- free** 7:23 8:4 72:10
freedom 82:14
Friday 73:20
friend 24:6 118:5,7
118:8
friends 24:18
frightening 71:5
front 8:8
FTC 21:24 22:6,19
73:4,10,25 74:12
FTP 38:2
full 35:4 51:2 52:10
53:10 85:6 87:11
99:10 110:22
112:15
function 28:22
29:10 87:22 123:4
123:9
functionality 55:6
functions 21:20
funded 14:3,6 15:12
15:15,18 16:14,21
17:15
funding 16:17,23
17:23 18:3,23
82:17 95:7
further 47:7 64:14
88:3 91:23 92:4
121:21 129:10
132:16
future 110:7
-
- G**
-
- game** 34:12
gap 60:23
gaps 81:20
gather 25:23
gathered 27:7 46:15
general 3:6 74:3
generally 23:23
53:23 88:18
generate 107:22
getting 64:6
Girl 33:6,7,14 55:12
55:15
give 6:4,13 21:10
27:18 37:13 40:23
62:11,17 77:17,25
82:14
given 19:22 37:17
41:3 67:10 78:3
85:14 86:23 87:4
87:23 88:12
- 113:17 132:15
glance 11:2
global 28:9 119:3,17
Gnutella 32:8,9
119:9 120:7,9
go 7:6 12:21 19:17
24:16,20 43:2,17
46:9 47:6 50:2
58:21 63:12 69:19
75:8 91:25 92:7
110:13 129:13
goes 47:22
going 4:12,14 10:13
24:19 28:4 45:9
63:3 67:3 90:7
93:2 118:16
122:20 126:6
128:10
Gomery 24:10
good 4:7 41:9 45:6
92:11
Gormley 24:13,14
41:24 61:24 79:5
79:21 80:10
117:22 118:8
Gormley's 117:25
gotten 55:19
governance 83:17
84:13,14 85:22
134:10
government 51:22
95:2,6
grab 63:20 64:21
graduate 20:18 21:3
grant 10:16 12:24
13:12 14:3,5,14,18
15:12,16,19 20:6
133:12
granted 18:23
graphics 21:20
great 24:17
greatly 70:5
Griffin 78:19 79:5
ground 7:7 8:12
group 20:3,11 87:21
groups 89:3
growing 34:20
119:13
guarantee 33:13
guess 13:16 15:12
37:13 89:21 90:4
guessing 42:7
guide 56:9,12
- guys** 4:16 63:20
64:21
-
- H**
-
- H** 1:16
hacker 90:24 91:2
116:7
Hampshire 3:8
hand 27:21,24
handed 45:14 61:15
67:19 75:4 78:11
83:22
Hanover 3:8
happened 24:3
happy 126:2
hard 37:25 109:24
harmful 39:9 51:12
51:15
hash 114:24,25
115:2,6,7,18
hashes 115:10
health 10:10 25:12
25:20 26:12 27:7
40:25 42:2 43:4,6
43:23 46:7,16,25
47:13 53:19 57:16
57:25 71:4,7 72:2
72:4 89:22 110:3
110:25 111:17
112:5 113:9,18
114:12
Healthcare 15:2
16:4 133:14
health-care 40:17
heard 94:8,10
help 7:18 46:12
115:18
helped 59:11
helpful 13:23 125:3
hemorrhage 16:3
65:25 126:21
133:14
Hemorrhages 10:10
15:2
hemorrhaging 17:7
17:12,20,25 18:11
18:20 20:15 22:25
24:22 26:10 37:2
68:5 69:2 80:22
89:16 99:8 103:4
110:19 128:19
Henry 1:16
hereinbefore 132:12

Hewlett-Packard 9:19	identities 104:20	49:20 50:25 51:18	informational 74:13	50:4,5
Hey 7:23	identity 25:21,24	52:11 56:3 59:12	Infrastructure 17:2	Ironically 112:16
high 25:13 81:19	51:21 71:14	71:3 89:18	initially 23:14 40:15	ISP 50:3
higher 4:19	108:12,13,14,15	indicated 16:12 18:2	initiate 12:23	issue 32:5 33:6
high-tech 26:12	108:16,22 109:5,7	19:7 29:7 37:4	initiated 12:9 13:10	issues 33:4,13
history 6:14 9:16	109:8,11,13,15,20	69:21 88:10	13:15 14:7,14	I3P 18:4,8
holders 32:3	110:4 112:6,23	103:18	25:14	
Homeland 10:4,16	113:13,25 114:2,4	indicates 70:4 73:16	initiating 12:20	J
11:8 12:3,10 14:18	114:7	76:3	initiation 23:12	J 3:12
16:15 18:9 19:3,10	II 2:10	indicating 49:17	insider 91:6,12,13	January 46:14
19:15,25 20:4,10	ill-intended 91:5	59:4 72:8 111:9	insiders 91:15	60:14
133:12	immediate 112:3,7	individual 35:23	insight 27:18	Jenio 1:18 132:8,23
Hopefully 129:20	impact 63:17 65:8	52:5 62:9 88:16,25	insights 70:5	job 16:20 52:15
Hopkins 78:18 79:9	implementation	101:16 102:18	inspecting 122:23	86:22 87:3,13
hospital 65:16 66:3	88:24	108:18,21 109:4	inspection 122:22	jobs 85:16
hospitals 25:15	important 7:10 8:7	109:19 110:10	install 25:15	Johnson 1:14 4:1,2
41:19 42:2,10	127:3	113:13,23 119:24	instances 100:15	4:7 5:1 6:1,23 7:1
43:18 62:8 109:17	impression 121:10	127:20,21,23	Institute 16:25	8:1 9:1 10:1 11:1
hospital-generated	inadvertent 23:19	individually 53:23	institution 43:7,15	12:1 13:1 14:1
52:12	25:4 38:12,16,17	individuals 38:20	47:24	15:1 16:1,5 17:1
host 57:3 59:22 60:2	86:16 89:20 90:23	39:9,10 77:4 89:3	institutions 17:19	18:1 19:1 20:1
60:4 67:3 123:4,9	90:24 96:11 97:4	96:10 109:15	25:5 26:8 43:13	21:1 22:1,21 23:1
hosts 57:4,9,15,23	97:14,18 98:7	112:2,16,23	46:17	24:1 25:1 26:1
58:6,11,24 127:18	108:3,7 112:4	116:18	instructed 77:16	27:1 28:1 29:1
hotel 50:3	116:6,12,17,24	individual's 112:5	insurance 46:6	30:1 31:1 32:1
house 69:16 70:20	inadvertently 5:24	industrial 6:9,10,12	59:17 103:9 104:5	33:1 34:1 35:1
housekeeping 93:5	35:7 97:10,22	industry 9:17 46:6	intended 5:20	36:1 37:1 38:1
HP 96:2	117:8	inevitable 89:20	intentional 26:24	39:1 40:1 41:1
human 82:6	incented 105:19	90:7,16	53:13 54:9,22 55:3	42:1 43:1 44:1
hypothetical 90:19	127:7	info 62:12	119:5	45:1 46:1 47:1
91:9,17	incentive 25:14	informal 8:6	intentionally 86:17	48:1 49:1 50:1
I	Incentives 83:19	information 11:14	interest 95:23 96:3	51:1 52:1 53:1
idea 55:2 71:25	84:15 134:12	11:20 17:2,5 22:10	96:24	54:1 55:1 56:1
85:13 100:9	incident 113:3	22:18 23:17 25:16	interested 13:14	57:1 58:1 59:1
ideas 17:12	include 6:15	25:24 27:8 34:2	14:25 23:16 55:23	60:1 61:1 62:1
identical 93:3 115:8	included 45:5 47:8	35:22 37:3,21	56:2,7 74:2 132:19	63:1 64:1 65:1
identifiable 52:13	93:11	51:24,25 52:4,13	interesting 57:13	66:1 67:1,15 68:1
71:12	includes 36:9	52:15 55:18 58:23	63:6	69:1 70:1 71:1
identification 4:24	124:18	59:3,17,22 60:2	interests 23:20	72:1 73:1 74:1,22
10:18 16:7 41:13	including 6:18 13:2	62:7 66:17,21	interfere 129:21	75:1,3 76:1 77:1
44:4 45:13 61:14	52:14 108:12	73:18 76:4 77:17	internal 82:2,7	78:1 79:1,2 80:1
67:18 74:24 78:10	128:12	78:3 83:17 84:13	Internet 119:13	81:1 82:1 83:1,22
83:21	incomplete 90:19	84:14 85:15,16,21	129:5	84:1 85:1 86:1
identified 60:4 66:6	91:9,17 92:6	86:15,20,22,23	interpret 71:22	87:1 88:1 89:1
66:10 105:9	inconvenience	87:5,24 89:22,24	interrupt 91:8	90:1 91:1 92:1,11
identifier 115:2	108:25	90:7,16 94:19 95:8	introduced 24:5,8	92:19 93:1,17 94:1
identifies 102:19	incorrect 71:22	95:25 96:6,12	92:12 118:7	95:1,22 96:1 97:1
identify 45:17 59:23	increased 47:9,10	97:10 98:20 104:6	intrusions 116:7	98:1 99:1 100:1
66:5 93:19 112:17	increases 100:20	108:5,8,17 110:25	invest 106:6	101:1 102:1 103:1
identifying 52:4	increasing 47:7	111:17 112:5,11	involved 22:24	104:1 105:1,12
106:19	INDEX 133:3 134:3	116:16,20,21,25	82:24	106:1 107:1 108:1
	indicate 28:3 40:12	117:7,11,13,15,16	involvement 82:22	109:1 110:1 111:1
	43:5 46:10 48:16	121:19 134:10	IP 49:5,10,19,25	112:1 113:1 114:1

115:1 116:1 117:1
 118:1 119:1 120:1
 121:1 122:1 123:1
 124:1,23 125:1,4
 126:1 127:1 128:1
 129:1 130:1 131:1
 131:7 132:11
 133:6,15,22 134:7
joined 8:25 9:4
joining 101:2
joke 118:5
journal 51:4
journals 98:24 99:3
judge 8:8 93:5
JUDGES 1:3
July 9:3,4
jury 8:9

K

keep 34:14 41:16
 119:12
Keith 78:19
Kevin 3:9 34:13,15
key 34:4,6 43:19
 116:16
kind 7:6 23:22 34:15
kinds 97:21
know 13:4 22:5
 23:23 24:17 35:5
 38:15 45:22 52:9
 58:19 60:3,6,7,9
 61:2,17 67:21
 68:11 75:5 78:13
 79:7,9 81:9 85:10
 93:13 103:16,19
 107:15,17,18,20
 107:21,25 113:7
 113:20
knowledge 29:17
 113:10
known 52:8
knows 34:5,15
Korn 1:16

L

lab 36:16,17,18
 59:15
labeled 103:6
LabMD 1:6 3:12 4:9
 74:8 92:16 94:8,16
 94:24 95:4,9
 103:12,15,18
 104:12 105:8

106:18 107:19
 114:14 117:18
 118:18,20 120:12
 121:9 123:3 124:2
 125:9
LabMD's 94:20
 116:5
laboratories 17:4
laboratory 9:24
 104:3
lack 91:4
lacks 30:24 79:23
laid 68:17
laptop 49:24 97:11
 97:24 117:12
laptops 117:10
large 53:12 60:23
 122:19

largest 40:22
latest 90:14
Laura 2:18 92:13
law 1:3 8:8
lawyer 5:4
lax 89:23
layman's 34:17,23
lead 110:6,8
leads 11:2
leak 40:24
leakage 71:3,6,9,21
leaked 40:15 57:12
 58:7
leaks 25:4,12,25
 26:7,11 89:25
learned 59:10
leaving 101:2
led 92:23 94:6,13
letter 4:22 68:17
 133:10
let's 6:13 14:23
 27:17 35:3 45:8
 46:9 53:9 58:21
 74:16 89:15
 108:15 114:4
 122:5

level 39:15 121:10
life 112:12,12
likelihood 100:18,20
LimeWire 31:25
 32:8 35:9 55:7
 56:24 120:5,7
 123:4,7
LimeWire's 55:4
limited 33:23

113:21 120:4
 126:2
limiting 116:18
line 80:9 99:10
list 34:10 40:16
 41:25 42:14,22,23
 45:7 81:19
listed 42:8,23 84:9
 124:22
literature 22:14
 96:15
little 33:2 34:14 47:7
 114:11
LLP 2:5
loans 109:3
locate 125:19
 126:13
located 69:23
 102:21 123:16
 127:17
log 50:3
long 23:5 84:6 110:8
 112:12
longer 23:7 61:7,8
 61:10 112:12
look 5:2 10:19 11:9
 12:21,22 13:4
 27:17 28:25 29:2
 44:6 45:8,16,21
 60:11,11 61:16
 65:22 67:21 69:19
 70:2,25 73:11 75:5
 76:2 89:15 118:22
 119:23 122:19

looked 94:23
looking 21:20 22:3
 27:10 29:24 32:17
 32:18 35:24 36:11
 36:14 37:14 80:2
 94:15,18 106:4,6
 111:7 124:8 127:9
 127:16 128:5,15
looks 34:12 42:20
 45:19,23 79:24
lose 97:11
loss 109:2
lost 97:24 117:9
lytec 107:12,13,15

M

M 1:14 4:2 131:7
 132:11 133:6
Madonna 33:5

55:12,14
Magazine's 40:16
Mail 2:16
mailed 37:17
main 3:7 31:6
maintaining 34:9
making 11:2 36:6
 123:16
malicious 108:18
manage 116:23
managed 90:25
 116:13
Management 9:14
manner 129:3
manual 115:15
manufacturing 9:25
manuscript 95:18
March 72:7 78:22
 79:21,24,24,25
 80:6,13,16
mark 4:20 10:14
 15:25 43:25 61:11
 93:3
marked 4:13,24 5:2
 6:2 10:17 16:6,10
 41:12,16,22 44:3,5
 45:10,12,15 61:13
 61:16 67:17,20
 74:23 75:4 78:9,12
 83:20,23 94:7,14
 99:7 103:3 106:9
 115:13 118:20,21
 119:16 129:16
marriage 132:18
masquerading
 109:12
Master's 6:10
match 33:9,10
matches 36:15
 42:22 47:9
material 33:6,7,14
 55:12,15 74:3,7
materials 74:14
 100:21
matter 1:4 72:22
 92:16 132:19
mean 22:8 31:20
 71:6 97:6 100:14
 105:2,24 111:23
 112:7 116:13
 119:7,18 120:24
meaning 71:20,23
 72:3 101:25

meaningful 21:8
means 28:14 121:2
meant 47:24 105:25
 119:19
measures 91:14,19
 128:17,23
medical 44:14 51:14
 51:21 59:14 62:6
 63:3,14 104:3
 107:3,12 108:14
 109:5,7,9,11,13,14
 109:19 110:5,7
 112:6 114:2,4,6
medicine 51:6
meetings 12:7 19:9
members 18:8,10
 20:3 82:12
membership 20:5
mention 22:23 43:3
 64:13 85:7
mentioned 20:19
 24:11 67:6 81:22
 119:9
mere 127:17
met 69:11,21 92:18
metadata 36:19
 45:23
method 40:11,13
 46:11
methodology 105:9
methods 37:20 38:4
Michael 3:12 34:13
 34:13
middle 62:5 80:4,7
mind 39:19 41:7
 71:25
mine 23:4
minute 110:14
mischaracterized
 111:13
mischaracterizes
 106:25
misconstrued 7:13
misdiagnoses 110:8
misstate 28:5
misstates 18:6 31:12
 57:19 58:18 59:8
 83:2 88:2,22
mistaken 116:11
 120:18
misunderstood 7:13
misused 100:19
moment 32:7 108:2

moments 102:12
 126:20
monitor 28:18
monitored 67:3
monitoring 28:16
 89:24 114:9
 119:20
monitors 28:9 119:2
 119:17
month 60:18 61:4,5
 61:6
months 8:24 9:2
 57:4,10 58:13 61:7
 61:10 67:4
morning 4:7 92:12
 92:18 114:13
 116:16 117:24
 123:2
motivated 106:5
mouse 105:5
move 8:16 53:9
 116:20
moved 53:12
movement 26:21
 98:19 113:11
moves 113:8
multiple 29:23,24
 31:8,10,14,17
 32:10,11 49:5,10
 49:16,19 100:15
 111:25 112:2
multiply 100:13,14
multi-year 12:24
music 38:21 55:8,9
 57:12
mutual 24:6 118:7

N

name 4:8 21:10
 24:10 27:21 36:17
 78:5,6,6,7 92:13
 117:25
named 26:7 27:3
names 43:18 47:2,3
Napster 34:7,8
national 96:17
nature 26:2 71:16
 71:25
near 47:4
necessarily 57:23
 58:14 62:7
necessary 76:7,16
necessity 88:24

need 7:23 36:19,21
 54:10 57:24 86:19
 87:2 89:23
needed 54:21 88:15
needs 85:15,17
 86:21 88:19
negotiations 12:7
net 53:13,24 57:25
network 28:19,20
 28:21,23 29:4,11
 29:22 30:3,11,12
 30:21 31:8,19,25
 32:6,8,9,12,21
 33:3,8,15,17 34:6
 35:22,23 36:7,10
 36:23 49:25 50:2
 67:7,12 77:15 78:2
 99:15,24 101:2,4
 101:10,17,20,23
 101:25 102:8,19
 104:22 106:3
 107:7 113:19
 115:17 120:7
 122:21 128:7

networks 25:7 26:4
 26:9,17,23,23,25
 27:16 28:10,16
 31:16,22 33:2,19
 34:4,18,20 35:9
 38:19 39:13,17
 40:6 46:13 54:12
 73:19 98:20 100:6
 100:22 119:3,9,18
 119:20,24 120:2
 125:21 126:18

never 102:3 110:11
 112:17
new 1:17,17,20 3:8
 68:19 132:4,6,10
newspaper 51:4
 100:10
next-to-the-last
 65:24 73:12
nice 8:15
Nicholas 21:11
NJ-3158 2:16
node 28:21 30:3
 31:8 102:16
nodes 30:4,5,6 31:17
 32:4,10 33:25,25
 55:6
nomenclature 30:7
nondisclosure

129:14
nonsensitive 117:16
notably 62:9
Notary 1:19 132:9
note 97:23 118:24
 127:3
noted 20:22 21:24
 129:25
notice 21:22 27:20
 81:18 86:2
noticed 22:21
November 44:11
number 4:15,19
 12:25 14:19 23:4
 27:23 33:23 47:8,9
 62:13 67:11 101:3
 112:13 117:19
 124:3
numbering 68:17
numbers 27:22
 52:15 59:16 93:6
 104:5 124:25
N.W 2:7,15

O

object 88:3
objection 18:5 26:18
 27:4 29:12,19
 30:14,23 31:9
 39:18 40:7 49:11
 50:19 55:21 56:11
 57:18 58:17 59:7
 62:20 70:11 79:22
 81:12 82:25 85:23
 87:25 88:21 90:18
 91:8,16 100:3
 101:11 102:9
 106:24 122:16
 128:22 129:19
objective 41:7
objects 92:5
obligations 110:9
observe 48:3,6
 125:20
observed 106:16
observer 29:14
obtain 109:13
obtained 95:8
obviously 52:19
occur 112:8
occurred 112:6,25
occurs 111:2,21
OFFICE 1:3 3:6

offices 1:16
Oh 23:2 66:13
 111:10 123:25
Okay 8:19 14:23
 15:17 21:2 22:15
 22:18 29:16 43:2
 48:11 61:21 63:12
 64:5,9,16 68:7
 75:22 89:6 91:22
 111:10 123:22
 124:2 126:4,8,24
ones 42:17 48:2 82:4
 119:12
One-page 4:22
 133:10
one-third 35:5
ongoing 82:22 83:5
open 41:16 108:18
open-sourced 33:20
operate 120:8,10
 128:7
operates 120:7
operating 32:7
opinion 85:25 90:20
 91:10,18
opportunity 19:22
 97:20
opposed 107:6
 121:11
order 76:7,16 77:18
 115:11
ordinary 121:18
organization 85:14
 88:20,25 90:13
 117:5 122:15
 127:24
organizations 44:23
 85:20 86:14 87:15
 87:21 122:11
original 34:16 44:25
 45:5 75:20 115:7
originally 99:21
ourself 54:13
outcome 132:19
outlined 15:20
outside 29:14
outsourced 66:2
O'LEARY 3:9 5:16
 13:19,22,25 68:12
 68:16 93:8 110:13
 111:8 129:12,20

P

page 5:16,17,22
 11:9 27:21,23 28:2
 28:3 35:3,4 38:11
 40:10 41:20,21
 42:9,19,21,24 43:3
 45:12,16,17,21
 46:2 47:4 48:15
 50:25 51:3 52:10
 53:10 62:5 64:21
 65:14,23 68:20
 69:4 70:2,25 72:5
 73:11,13 75:8
 78:18 80:4,7 85:5
 85:7 87:10 89:18
 99:9 103:5,7,11,24
 104:2 105:7,11,12
 105:14 106:9,21
 110:18 111:16,19
 112:15 113:16
 114:16,24 115:12
 124:4,5,6,10,13,17
 124:24 126:21
 133:5,9,19 134:5
pages 10:25 61:16
 73:13 84:6,8 93:13
 124:3,14
PAGE/LINE 130:6
paid 80:25
paper 20:20 21:19
 28:6 37:9 38:10
 43:12 53:8 56:21
 60:10 73:5 84:3,4
 84:6,8,12,21,24
 85:2,6,11 86:2
 87:7 88:5 90:22
 93:24 94:4,7,14
 95:13,18 99:8
 103:4 104:2 105:7
 110:20 113:16
 114:24
papers 25:8 39:22
 97:9
paragraph 35:4,6
 46:10 47:5 51:2
 52:11 53:10 59:12
 65:15 76:2 85:6
 87:11 88:7,11
 99:10 103:25
 104:19 105:15
 110:22 112:16
 114:20
paraphrasing 87:19
 114:22

- part** 9:23 10:23
 11:17 16:20,22
 17:15 18:12 19:15
 38:17,24 84:4
partially 15:18
 16:14
participate 12:15
 17:6,8 28:20 29:21
 30:3,11,21,25 31:7
 74:12 119:25
participated 12:13
 19:8 21:7
participating 74:6
 101:17,19,23
participation 82:19
particular 21:5,6,9
 23:18 45:24 46:2
 52:25 57:2 60:8
 66:9 67:11 86:9
 96:23 101:7 102:5
 114:2,6 117:21
 119:21 122:21
particularly 39:22
 45:16 97:17
parties 132:17
partner 23:4,9
partnered 125:23
 126:16
partners 81:14
partnership 83:5
parts 32:11 78:5
party 36:11
passed 33:7,11,15
 33:23
password-protected
 129:6
patent-pending 28:8
patient 59:16 104:4
 104:20
patients 59:18 104:7
 113:4
patient's 113:12
patterns 26:5
Pause 61:20
pay 110:11
payers 109:16 110:9
payments 25:15
peer 20:2,5,11
peer-review 19:18
 19:19
peer-reviewed
 96:15 98:24 99:3
peer-to-peer 25:7
 26:4,5,9,17,22
 31:16 35:8 39:12
 39:17 40:5 97:19
 97:25 98:2 106:15
 107:7 117:4
 122:13 125:20
 126:18
Penn 6:8,10,11
Pennsylvania 2:7,15
people 51:15 79:7
 87:21 102:2
percent 48:16
Perez 1:18 132:8,23
perfect 90:10 91:14
 91:20
perform 21:19
 32:12 87:12,22
performed 103:20
 103:21
period 13:3 15:19
 46:14 60:18 62:19
periodically 57:4,9
 58:12
permitted 76:3
personal 52:4 71:11
 71:16 94:19 96:12
 108:4,8,17 110:25
 116:25 117:14
personally 52:13
persons 20:16
person's 21:10
 109:8,13
pervasively 122:10
phase 37:5 42:11
 56:15 62:25 63:10
 64:7,11,13 65:3,3
 65:4,5 79:15 80:21
 106:22 120:14
phases 50:16
PHI 110:23 111:7
 111:14,15,19,24
 113:8
phone 23:25 74:5
phones 117:10
Ph.D 1:14 4:2 6:11
 131:7 132:11
pictures 38:21
piece 36:8 116:17
pieces 17:17
pile 123:24
place 41:5 75:19
 82:9 98:3 111:6
 128:18
placed 109:4
places 31:24 77:13
planned 38:23
please 4:21 10:20
 32:20 43:3 44:2,8
 45:9,18 46:9 48:24
 61:16 72:12 75:4
 78:12 85:12 92:7
 93:18 103:2
 123:23 129:24
PLLC 1:16
plugged 49:24
plural 26:24 119:4
 119:18
point 4:17 47:12
 70:18 92:4 101:3
 118:24
pointed 119:4
 126:25
policies 89:2 90:14
popular 35:8 119:8
portability 89:19
portion 17:23
 103:17
ports 117:12
posed 122:7
position 40:3 90:15
positive 47:11,15
positives 47:11
possibility 74:6
possible 38:22 50:12
 66:11,12
possibly 38:7 41:6
 56:10 65:20,21
 69:18 80:3
post 25:13 26:12
Posts 57:12
potential 39:10
 53:25 73:21,23
Potentially 61:8
practice 85:20
practitioners 62:9
preceding 103:24
precisely 36:14
predicated 95:7
prefer 6:25
prepared 18:7 96:8
present 3:12 81:7
presented 93:24
 96:17
Presumed 38:17
presumption 38:24
 39:2,5
pretty 8:17
Preventing 91:2
previously 4:17
pre-publication
 84:25
primarily 15:24
 33:20 38:20
printed 37:16
prior 9:9,18 12:20
 13:2 23:6 31:13
 57:19 58:18 59:8
 64:2,6 75:19 83:2
 88:2,22 92:23 94:6
priority 81:19
private 117:14
privileges 87:14
 88:13
probably 76:12 85:2
 123:24
probing 44:14
problem 98:5,6
 109:25
problems 97:4
procedures 90:15
proceeding 92:4
process 19:6,11,18
 19:20 20:7 62:24
 77:6 79:13 125:10
productivity 82:13
professional 122:12
professionals
 121:20,24 122:7
professor 6:16 9:11
 92:19
professors 82:10
professor's 16:20
program 25:14
project 17:18 25:3
 26:11 83:11,12
projects 25:19,22
 26:7,14 27:3,7
 82:3,8,13
promising 57:5
 58:13
proposal 12:10,12
 12:16,19 13:13
 14:2,15 17:14 18:3
 18:7,12,16,16,21
 18:24 19:6,11,13
 19:14 20:6,10
proposals 19:16
protect 41:5 86:16
protected 111:16
 112:5 128:24
protection 2:14 17:2
 82:6
protocol 40:21
provided 19:20 20:6
 22:10,19 38:2 84:7
 85:16
providers 40:23
 113:9
provides 52:4 55:7
psychiatrists 62:10
public 1:19 74:3,14
 122:3,6 132:9
publically 120:21
publication 84:19
 95:20
publicly 36:6 40:17
 43:4 120:24
 123:17
publish 103:22
published 10:11
 15:9,10 22:3 35:8
 81:23 96:15 99:2
publisher 51:14
pursuant 1:15
put 19:9 53:5 75:19
 97:12
puts 89:3
p.m 129:25
P2P 28:9 46:13
 73:19 78:2 96:24
 98:9,20 99:11,14
 99:24 100:5,21
 101:10 102:8,19
 104:21 106:2
 115:17 119:3,17
 121:11,16 122:8

Q
qualify 54:10
question 7:16,25 8:2
 13:20 29:6,8 30:20
 47:24 50:22 54:16
 54:24,25 58:20
 114:23 118:18
questions 7:15
 89:14 91:23
 106:18 114:14
 117:19 124:3
 126:5
quick 62:12 98:16
 126:7
quickly 8:17 34:11

110:3 115:23
quite 8:21
quote 110:25 120:20

R

random 37:7
randomly 46:15
range 82:15 108:24
reach 102:3,16
read 28:4,10 35:14
46:19 51:8 52:17
53:16 57:6 58:22
59:19 62:14 63:21
76:10 87:17
104:10,24 105:22
111:5 129:23
reading 61:18
reads 53:11 104:19
ready 75:7 78:13,15
real 109:2
realize 112:18,25
113:14
realized 122:10
really 28:14 39:23
53:6 56:4 63:17
65:8 98:3
real-time 28:9
reason 14:16 125:22
127:17
reasonably 76:6,15
reasons 101:15
recall 15:22 24:7
61:3 69:25 73:9,25
74:11
receive 49:25 87:13
110:4
received 60:7 64:17
110:12
recently-hired
52:14
Recess 74:19 89:11
115:25
recognize 83:24
84:8
recollection 44:25
70:8 75:23 78:7
record 48:24 72:11
72:13 84:5 91:25
92:7,8 93:2,18
110:5,14,16
129:13 132:14
recorded 21:23 22:7
records 83:14

redacted 103:10,17
redaction 103:20,21
redirect 126:2
refer 27:23 104:12
114:19
reference 86:3
referenced 22:12
65:18 73:6
references 21:21,23
114:15
referencing 80:20
124:24,25
referred 17:14
referring 16:9 70:13
79:10,12,17
110:24 112:21,22
refers 111:16
114:24
refresh 70:7 75:22
regard 12:4 22:6
39:12,16
regarding 62:12
96:9
related 11:19 14:20
21:18 22:3 25:8,9
34:25 36:22 43:12
43:15 46:16 55:14
63:20 64:22 69:12
94:16 132:17
relating 117:20
relation 69:15
relationship 81:4
124:14
relatively 68:19
release 63:19
relevant 119:21
remember 69:5,9
98:10 114:16
116:8 117:25
120:15,21 121:13
123:4 125:13
remote 37:18
remotely 38:3
removing 117:12
replaced 93:20
reply 80:2
report 32:16 42:18
49:3 54:7 63:5,15
63:17,19 65:8 68:4
68:5 72:24 103:10
103:11
reporter 1:19 7:8,19
8:15 10:14 132:9

represent 4:8 42:9
representatives 76:5
represents 42:4
107:5
requester 34:16
requesting 68:24
research 10:5 12:4
14:3,5 15:13 16:18
16:21 17:5,11
18:18 19:21,21
21:18,25 22:6 23:3
23:9 24:21,25 25:6
25:10 26:20 27:9
27:12 38:12 39:6
39:13,21 40:11,13
40:20 42:11 46:11
53:5 55:17 58:8
60:5 62:16,19,21
64:3,7 72:9,15,25
73:2 75:17 80:21
81:2,14,16 82:3,8
82:9,12,15,18,19
82:24 83:5,10
85:18 86:5,10
92:23 94:6,13,22
95:7,13,24 98:15
105:9 106:12
118:13 119:22
120:14 121:22
125:23 126:17
researchers 17:19
107:6
reside 102:15
resident 121:4
resold 111:2,20
resource 22:13
respect 17:11
113:12
respond 7:10 8:2
19:22
respondent 1:15 2:6
92:2
response 29:3 69:4
80:15 118:17
123:2
result 10:8 18:21
resulted 95:13,18
120:14
results 64:7
retrieve 49:15 99:18
return 102:25
123:22
review 20:3,5,11

22:14 38:3 63:24
78:12 82:2,8,9
95:17
reviewed 61:17
67:22 75:6 98:23
reviewing 62:24
reviews 19:19,23,24
82:11
RE-EXAMINATI...
126:10
re-share 100:7
re-shared 99:24
right 8:10 11:2
27:21,24 51:17
59:6 62:14 63:5
80:17 81:17 111:6
118:11 124:20,21
right-hand 124:22
right-most 107:10
ring 24:15
Riposo 2:18 5:7,12
18:5 26:18 27:4
29:12,19 30:14,23
31:9,12 39:18 40:7
41:8 49:11 50:19
53:2 55:21 56:11
57:18,21 58:17
59:7 62:20 67:23
68:7 70:11 74:18
76:9 78:24 79:22
81:12 82:25 85:23
87:25 88:21 89:9
90:18 91:7,16,24
92:10,25 93:15
110:15 115:20
116:3 125:25
126:8 128:22
129:11,18 133:6
risk 96:9 99:13,16
99:19,23 100:2
risks 39:10,24
121:11,16 122:7
road 4:18
role 21:15 88:10,12
88:14,16 89:5
92:15
roles 6:17 87:16
88:12
role-based 88:8 89:3
rooms 129:8
roughly 87:13,22
rule 85:7,9 86:3,6,11
86:13 87:3,20 88:9

88:18,23
rules 7:7 8:13 90:14
run 96:7
running 102:22
122:24
runs 102:18
RX 4:15 67:20 133:9
134:5
RX-1 4:17,21,24 5:2
6:2
RX-10 78:10,12,16
RX-11 83:20,23
88:6 92:3
RX-2 10:15,18,19
16:13 17:15 22:21
23:2
RX-3 16:2,6,10
26:10 27:17 35:3
42:21 43:3 46:9
48:16 65:15 89:15
93:4,10,11,14
118:20
RX-4 41:13,17 42:9
42:24
RX-5 44:4,6
RX-6 45:8,10,12,15
RX-7 61:14,16
63:25
RX-8 67:17 68:20
73:12
RX-9 74:23 75:4,8
123:23 124:2,7,10
124:13,15,18
129:15
résumé 68:12

S

safe 38:25 39:5
salary 16:22
sample 40:14 46:15
48:13 59:10
sampling 37:7 53:12
58:24 59:3
Samuel 78:18
satisfied 55:18,22
saved 99:20
saying 33:18 66:16
90:4,5,6,6
says 47:5 58:23 62:6
63:2 64:21 65:24
79:10 127:3
scenario 50:14
school 6:17 9:8,14

Schultz 78:19 79:6	133:12	shared 39:8 46:15	31:2 55:9 96:8	speed 34:2
Science 6:8	see 11:11,15 17:16	48:2 50:10 52:6	simple 109:12	spent 81:15
scores 114:9	21:12 32:2,11 33:8	56:25 57:5 58:13	single 29:22 32:13	spice 63:15
screenshot 103:10	35:11 36:5 43:8	58:15,24 73:8 78:2	32:14 38:9 104:21	spoken 92:21
search 26:5 31:23	44:16 46:8,17	100:5,21 117:8	115:4	spread 49:4,9,18
31:24 32:5,5,13	53:14 55:10 62:22	121:2	six 8:24 57:10 58:12	spreadsheet 45:11
33:4,6,13,22 34:3	64:13,24 69:7	sharing 11:14,20	61:9,10 67:4	45:20 52:12 65:16
34:24 35:2 43:22	81:15 97:21 104:7	17:11 25:7 26:4,6	sixth 60:18	133:18
45:2,25 54:9,11,12	104:22 105:19	26:16,22 27:12,15	Six-page 67:14	spreadsheets 36:18
54:22 55:11 56:17	111:3,10 112:19	28:10,16,19 31:16	133:21	squarely 46:7
56:22 77:7,8,20,21	123:11 128:10	35:9,20 36:4,10,23	size 37:21 115:3	ss 132:5
95:3 101:6 102:3,4	seen 5:4,10,15,25	38:20 39:12 40:5	skimming 22:22	staff 95:12,17
102:16,18,19	10:21,23 11:3,22	51:15 55:11 56:24	skips 67:24 68:8	stage 53:11 55:16,19
106:13,14,18,20	segments 88:11	57:12 73:10 74:4	small 72:4	57:15 58:4,8,16
106:22 107:5	segregating 117:13	86:16,16 96:24	Social 52:14 59:16	60:5,13,17,19,24
115:16 123:14,16	self-evident 48:22	97:19 98:2,3 101:5	104:5	60:24 62:16 64:2
searched 46:12	66:14	106:2,15 114:10	softball 24:19	80:21
67:12 120:13	sell 111:25	117:4 119:3	software 107:16	stamped 16:5 67:15
searches 26:25 27:2	sending 34:3 72:7	123:12 125:20	sold 111:2,20	74:22 133:15,22
27:5,8,10 53:14	sense 50:24 52:3	126:17 128:9	solely 15:15	134:7
55:3 63:20 64:22	97:17	Sheer 2:19 4:16	song 33:5	stands 111:14
106:11	sensitive 73:18	72:15 92:17	songs 36:16 55:10	Stanford 6:12
searching 32:14,22	94:19 99:13,23	Sherman 2:10 4:6,8	55:14,14	start 61:22 62:3
32:24 35:11 36:16	100:18 116:25	4:14,20 5:9,19	soon 100:9	108:15 117:5
36:20,21 53:24	117:7,15	13:21,24 14:4	sophisticated 41:4	starting 4:19 6:5
54:14 55:8 56:14	sent 5:5 41:24 79:20	15:25 41:11,15	sorry 23:2 61:19	starts 88:18
second 40:12 45:16	80:8,16	43:25 45:8 61:11	76:9 78:24 79:3	state 1:19 6:8,10,11
46:10 53:10,11	sentence 35:6,12	68:3,10,14 72:11	91:7 111:11	39:19 65:6 91:25
55:16 60:18,24	40:13 51:2 58:21	74:16 75:2 76:12	source 22:11,13	132:4,10
87:10 101:18	59:2 64:20 65:22	79:3 89:6,13 91:22	50:18 52:7,24 53:3	statement 10:6
105:15 110:22	65:24 71:20,22	98:9 100:3 101:11	53:7 66:6,9 113:24	35:16 36:2 127:2
112:15	87:10 104:18	102:9 106:24	sources 16:18,23	states 1:2 11:10
secondary 22:13	105:15 110:23	122:16 126:4,9,11	50:10,14 53:5 66:5	87:11 104:2
secondly 7:14 54:15	111:14 118:25	129:9 133:6	66:11 82:17	stem 109:19
129:5	119:14	shipped 37:24	South 3:7	step 54:17
section 40:13,23,24	series 11:6 25:19	SHOHL 2:5	space 115:5	steps 54:19,21
46:11	27:22 61:23 76:23	short 41:19	spanning 25:20	stolen 112:18
sector 10:10 15:3	server 38:2	Shorthand 1:18	speak 73:20	113:15,20
16:4 25:13 26:12	services 114:9	132:8	specific 14:17,21	Stop 2:16
27:6,7 40:25 71:4	serving 92:15	shortly 60:20	18:17 26:16 36:20	stored 129:7
71:7,9 114:12	set 34:25 51:19	show 4:12 10:13	41:7 53:13 54:5,8	strategies 6:19,20
133:14	63:25 87:14 88:13	45:9	54:22 55:2,6 77:7	street 1:17 3:7 24:3
sectors 77:9 86:8	120:9 122:5	showed 117:19	77:8,21,23,24	string 33:7,11,14
secured 129:7	132:12	showing 4:25	113:3 115:17	34:22 41:12 44:3
security 10:4,16	sets 40:10	shown 44:5	specifically 20:23	67:15 78:9 110:9
11:8,13,19 12:3,11	setting 8:6	sic 24:10	23:24 26:3 54:16	133:16,17,21
14:19,20 16:15	Settlemyer 68:21	sided 73:14 74:20	94:15,18,23 99:8	134:9
17:5 18:9 19:3,10	69:5,10,21,23 70:3	134:6	117:15	strings 77:20,22
19:15,25 20:4,11	70:10,16 71:3 72:6	sign 129:24	specifically-tailored	structure 31:15
52:15 59:16 90:11	72:15 73:14	signature 46:13,21	89:2	students 20:18 21:3
91:14 93:25 104:5	124:19 125:5	46:24 53:21 63:21	speculation 81:13	51:6
121:19,24 122:6	share 31:23 37:21	64:22 65:2 124:18	101:12 102:10	study 37:6 46:5
122:12 128:17,23	38:22 63:13 89:4	similar 28:25 29:2	122:17	50:17 97:17,18

98:4 106:23
126:22 128:20
studying 23:16 51:6
stuff 63:6
subject 42:10 44:14
72:22 73:22,24
80:9 125:25
subjects 82:6,9,15
submission 20:9
submit 84:5
submits 20:11
submitted 18:8
19:14
subnetworks 32:11
subpoena 1:15 4:9
4:23 5:6 133:10
Subscribed 131:9
subsequent 25:12
62:23 69:22 83:12
subsequently 27:14
77:14 79:20
substantial 21:8
125:19 126:13
127:12
subtleties 34:19
successfully 32:2
suggest 54:19,20
suggests 59:2 87:4
suite 2:8 3:7
summer 60:21
super 33:25 34:5
sure 13:21,24 14:22
23:11 30:16 41:11
42:13,16 45:6
50:21 74:18
115:19,24
suspect 5:9 71:8
switch 126:6
sworn 4:4 131:9
132:13
symptom 89:25
synonymous 34:23
system 37:18 41:4
110:2 113:10
114:8
systems 89:23 96:7

T

table 8:2
Tagliaferri 78:19
79:5
tailored 88:19
take 5:2 7:19,22,24

35:21 41:9 45:15
50:7 54:19 67:21
74:16 75:5 82:10
89:6 91:20 115:21
118:22
taken 1:15 7:4 10:19
54:21 91:14 99:21
talk 7:21 108:2
talking 14:13 41:18
62:23 64:11 65:15
taste 55:9
team 19:21,21 47:21
53:4 54:12,18 77:4
team's 55:2
tech 25:13
technical 34:19
technologies 117:10
technology 24:23
25:16,23 26:15,21
28:8 29:8,9,18
30:10,19 31:5 37:2
37:23 49:14 56:13
76:8,17,19 81:2,11
90:14 95:25 98:9
98:17 119:2 120:4
125:11,17 128:12
Telephone 12:6
tell 8:9 44:7 48:23
50:13
tellers 87:12
ten 6:14,15 8:20,21
40:16,19 41:3,18
41:25 42:6,9,15
43:4,23 44:23
53:19,22 57:16,24
112:15
tender 126:3
tenets 82:14
ten-minute 74:17
term 14:8 34:22,23
106:14 107:12
terms 10:17 12:8
18:17 20:14 28:15
31:18 36:25 39:16
43:12,14,21 44:15
44:19,20 45:2,3,5
45:25 47:8 50:17
53:19,22,24 54:4
85:21 86:6 106:19
106:20,22 107:3,6
133:12
Terrific 125:2
Testificandum 4:23

133:11
testified 4:4 66:4
69:12 96:20
126:21
testify 69:14 78:13
85:12
testimony 13:9 18:2
18:6 31:4,13 42:22
57:19 58:11,18
59:8 63:7 69:20
70:20,22 83:2 88:2
88:22 98:10
106:25 114:17
116:8,11 120:15
120:18,22 121:13
123:5 125:14
132:14
testing 59:15 104:3
text 34:25 104:8,22
105:20 111:3
112:19 114:15,23
textbook 51:14,16
thank 5:12 8:19
60:16 89:10 93:15
125:3
thanking 72:7
theft 25:21,24 51:21
71:15 108:12,13
108:14,15,16,23
109:6,7,11,15,20
109:22 111:2,20
112:6,17,24
113:14,25 114:3,5
114:7
things 5:14 25:25
59:10 81:20
116:22 117:2,6
think 4:18 5:13,17
8:14 17:25 19:7,17
20:18,23 21:5
22:12 24:5,10,12
25:18 29:14 38:6
38:25 39:4 41:6
42:5 46:4 54:23
68:12,16 70:13
71:23 73:5 74:4
78:6 79:12 86:13
93:12 111:13
115:22 118:5
121:21,21,23
122:9 124:24
126:9
third 47:4 99:10

107:11 110:22
119:11 129:7
third-party 128:25
thought 14:9,11
thousands 59:18
104:7
three 23:7 48:11
Three-page 61:13
133:20
Thursday 73:20
time 6:15 7:22 8:4
13:3,13 15:19
18:16 37:23 39:5
41:9 60:9,10 62:19
67:10 69:12 70:19
72:10 73:20,25
81:15,21 85:3,18
86:9,12 101:3,17
101:20,23 121:24
129:25
times 31:8 49:16
66:20 111:25
title 11:13 36:18
101:7 102:5
titled 16:3 133:13
Tiversa 22:23,24
23:3,8,15,20 24:2
24:4,7 25:10 26:15
28:7,15,18 29:10
29:23 31:7 32:16
32:24 37:15,16
46:12 47:20 48:7
54:13,17,19,20
56:2,3,6 58:20
60:8 64:14 65:12
67:5 75:11,24
77:16,18 78:3 79:8
80:10,24 81:4,10
81:22 82:4,22 83:4
83:11 106:16
117:21 119:17
125:7 126:12
127:25 129:15
Tiversa's 24:23
25:23 30:10,19
31:5 36:25 37:18
76:19 82:18 119:2
120:3 125:11,17
127:11
today 75:18 90:12
92:15,17 98:8
101:7 106:17
116:4

told 23:22 63:15
65:6,10
tons 62:8
top 27:20,24 40:16
40:18 41:3,18,25
42:6,9,15 43:4,22
44:23 53:19,22
57:16,24 80:16
103:18
total 25:18
track 98:19 110:10
113:2,24
Trade 1:2 2:13
92:14 95:11,16
124:20
traded 40:17 43:4
traditional 71:13
traffic 122:20
trail 34:14
train 97:12
transcript 8:16
transfer 37:23
117:11
transferred 37:14
transfers 26:3
translate 7:20
treasure-trove 62:6
treatment 59:17
104:6 109:14
110:5,11
troublesome 91:3
true 50:16 51:10
85:4 90:12 102:14
132:14
truly 50:13
Trustees 11:7
truth 8:9
try 8:13 14:23
110:10
trying 50:17 53:6
Tuck 6:17
turn 35:3 41:20
65:14 72:5 85:5
103:5
turned 63:5 128:9
two 23:6 38:4 50:5
60:13 61:7 65:16
72:21 73:13
101:15 115:6
Two-page 44:3
74:20 78:9 133:17
134:6,9
two-week 46:14

type 21:24 51:3
55:18 56:16 91:2
107:16
typed 106:15
types 43:21 71:10
109:11
typical 29:21 30:12
30:12,15
typically 20:3 31:22
33:16,22 38:8

U

uh-huh 7:12
um-hmm 6:21 7:12
uncover 54:6
uncovered 59:13
understand 8:10
30:16 51:17 60:12
understanding 10:2
20:8 28:13 30:19
31:5 32:19 98:13
98:14
understood 29:7
undertake 105:19
127:7
uniform 88:13
unique 47:2 93:6
115:2
UNITED 1:2
universities 17:3
university 8:25 9:12
16:21
unrelated 47:13
54:6
unsigned 75:10
unusual 97:3,7
upper 124:22
use 29:23 31:14
43:22 63:14 80:25
81:10 92:3 108:17
109:8 117:4
126:23 129:22
user 26:24 27:2,5,8
27:10 28:23 29:4
29:11,15,21 30:13
30:22 31:24 32:13
32:14,17,21,25
33:4,5,10,11,12,13
34:3,5,10 36:3,15
36:23 49:15,21,23
57:2 99:20 100:16
101:19,22,24
105:4 106:16

120:20 123:7,10
123:11,12,13,15
123:19 127:20,21
users 26:6,17 29:24
30:6,25 31:19,23
32:6 33:8,24 36:9
38:22 39:16,20,24
40:4,8 55:7 58:6
67:11 77:12 99:11
100:25 101:3,5
107:6 119:24
120:4 127:23
user-issued 106:11
106:12
uses 37:11
usually 8:12
utilize 25:23
utilized 128:19

V

vague 27:5 29:20
30:15 39:19 40:8
50:20 53:2 54:5
55:22 56:12 57:21
62:21 81:13 85:24
100:3 128:23
value 111:24
valued 81:15
Van 2:18 5:7,12
18:5 26:18 27:4
29:12,19 30:14,23
31:9,12 39:18 40:7
41:8 49:11 50:19
53:2 55:21 56:11
57:18,21 58:17
59:7 62:20 67:23
68:7 70:11 74:18
76:9 78:24 79:22
81:12 82:25 85:23
87:25 88:21 89:9
90:18 91:7,16,24
92:10,25 93:15
110:15 115:20
116:3 125:25
126:8 128:22
129:11,18 133:6
Vanderbilt 8:25 9:5
9:11
VanDruff 92:13
variety 128:11
various 6:17 21:19
86:8 108:12
vary 100:22

vast 127:24
verbal 65:9
verbally 7:11
version 85:2
versus 90:23
victim 108:11
video 32:16 38:21
view 47:12 97:3,7
123:14
viewed 29:15 100:6
virtue 5:6 58:15
Visa 112:12
vitae 25:8

W

wait 7:15,17
want 14:22 23:23
55:10 85:5 86:15
91:25
wanted 45:6 55:20
90:17 123:8
wants 33:5 93:6
Washington 2:9,17
wasn't 8:20 15:15
22:18 66:5 68:15
79:18
way 19:9 21:7,8
29:5 31:2 35:5
71:22 95:12
107:11 120:13
121:7 132:18
ways 42:15 48:12
71:5,17 97:9
weeks 60:13,23,25
61:4
went 16:19
weren't 39:25 66:11
81:19
we'll 7:24 8:16
50:23
we're 4:14 14:13,22
16:8 59:9 62:23
88:7 112:22
we've 41:16 62:8
124:24
whispering 34:12
wide 82:15
widely 85:24 86:6
86:11
widely-acceptable
85:19
widespread 114:10
Willey 21:11,17,25

22:5
Willey's 21:15
William 2:10 4:8
41:8 89:10
wind 100:8,11,12
wish 7:22 38:22 52:5
wishes 92:3
wishing 99:17
witness 4:3 88:4
115:24 129:23
132:12,15 133:5
wonder 24:11
word 91:5
words 37:12 115:6
work 11:18 12:9,20
12:23,25 13:9,15
13:17 14:2,5,7,14
15:15,20,22 16:18
17:4,10,20 22:16
22:17 23:6,21 25:9
25:11 34:18 37:13
39:11 40:21 49:25
50:2 69:13,15 70:6
70:10,14,17 73:21
73:23 75:20 86:3
96:2 117:3
worked 9:17,18
17:10 20:16
working 9:24 35:23
63:4 66:2 75:24
84:3,4,20,24 88:5
works 27:19 29:18
87:14,20 98:9
world 77:13
worthiness 114:11
wouldn't 117:9
wrap 115:22
write 62:11
writers 20:6
written 10:11 19:13
79:18 90:14
wrong 32:21 49:20

X

x 1:3,8

Y

Yeah 14:10 20:22
26:3 42:5,5 75:7
year 69:17
years 6:14,15 8:20
8:22 12:25 14:19
23:4,7 83:15

York 1:17,17,20
132:4,6,10
Yup 27:25 42:3,20
42:25 44:13
111:10 126:24

Ü

über 33:25

0

000001 67:16
133:22
0000010 99:9
000003 16:5 133:15
000023 74:22
124:23 134:8
03755 3:8

1

1 4:13 28:4 41:22
56:15 57:15 62:25
63:10 65:3,4,5
80:21,21 106:22
118:19,22 119:15
120:14 124:5,6,13
124:17,24 133:10
1st 9:3,4
1,718-page 59:15
74:9 104:4 107:22
10 40:10 43:3
113:16 129:16
133:12 134:9
10-minute 115:21
10017 1:17
11 42:19,21 47:4
48:15 114:16,24
115:12 134:10
12 50:25
126 133:6
13 52:10 53:10
103:24 104:2
14 103:6,7 105:7
15 65:14,23
16 133:13
17 105:11,12,14
126:21
18 1:8 78:22 79:21
80:13 106:9,21
130:2 133:2 134:2
18th 79:25
19 44:11 89:18

2

2 46:2 48:15 64:2,7 64:11,13,21 65:3 67:16,25 69:4 114:20 124:4,4,14 133:12,22	34 67:17 133:23 382 93:23
2:00 129:25	4
2000 4 2:9	4 35:3 40:13 41:22 46:11 87:10 103:7 103:8,9 104:16 107:23 111:16 124:14 129:16 133:10,16
2005 23:10 75:20,23 81:5	41 133:16 42nd 1:17 44 133:17 45 133:18
2006 69:18	5
2006-CS-001-000... 11:11	5 44:2 65:23 72:7 129:16 133:17 50 48:16
2007 13:2,11 44:11	6
2008 13:2,2 15:24 39:14 40:2 46:14 60:15,16 62:3,17 65:19 78:22 79:21 80:13,16 83:19 84:18 102:4,14 121:17 134:12	6 133:18 600 2:15 61 133:20 610 2:8 63 3:7 67 133:21
2009 13:3 15:10 39:14 68:22 72:7 83:13 94:2	7
2010 73:15 83:13	7 61:12 129:16 133:20 74 134:6 78 134:9
2013 9:4	8
2014 1:8 130:2 131:11 133:2 134:2	8 67:20 73:15 106:10,21 107:2,5 110:18 111:19 133:21 801 2:7 83 134:10
20580 2:17	9
21 67:16,25 93:13 133:22	9 134:6 9,000 104:20 9:55 1:9 92 133:6 9357 1:5
22 67:16,25 70:2,25 133:22	
220 1:16	
24 16:6 75:8 83:19 84:18 133:15 134:12	
26 74:23 80:16 134:8	
26th 80:3	
27 67:16 68:8 72:5 133:23	
29 62:3,17 65:18	
3	
3 28:2 51:18 68:22 85:5 93:13 124:14 133:6,13	
3rd 70:4	
3(a) 76:2	
3,328 37:6 48:14,17	
30 84:6	
301 3:7	

Exhibit B

Data Hemorrhages in the Health-Care Sector¹

M. Eric Johnson

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

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

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

1 Introduction

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

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

Given the highly fragmented US health-care system, data hemorrhages come from many different sources—ambulatory health-care providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back-offices of health maintenance organizations, and outsourced service providers such as billing, collection, and transcription firms.

In this paper we analyze the threats and vulnerabilities to medical data. We first explore the consequences of data hemorrhages, including a look at how criminals exploit medical data, in particular through medical identity theft. Next, we examine types and sources of data hemorrhages through a direct analysis of inadvertent disclosures of medical information on publically available, internet-based file sharing networks. We present an analysis of thousands of files we uncovered. These files were inadvertently published in popular peer-to-peer file sharing networks like Limewire and Bearshare and could be easily downloaded by anyone searching for them. Originating from health-care firms, their suppliers, and patients themselves, the files span everything from sensitive patient correspondence to business documents, spreadsheets, and PowerPoint files. We found multiple files from major health-care firms that contained private employee and patient information for literally tens of thousands of individuals, including addresses, Social Security Numbers, birth dates, and treatment billing information. Disturbingly, we also found private patient information including medical diagnoses and psychiatric evaluations. Finally, we present evidence, from user-issued searches on these networks, that individuals are working to find medical data—likely for malicious exploitation.

The extended enterprises of health-care providers often include many technically unsophisticated partners who are more likely to leak information. As compared with earlier studies we conducted in the banking sector (Johnson 2008), we find that tracking and stopping medical data hemorrhages is more complex and possibly harder to control given the fragmented nature of the US health-care system. We document the risks and call for better control of sensitive health-care information.

2 Consequences of Data Hemorrhages

Data hemorrhages from the health-care sector are diverse, from leaked business information and employee personally identifiable information (PII) to patient protected health information (PHI), which is individually identifiable health information. While some hemorrhages are related to business information, like marketing plans or financial documents, we focus on the more disturbing releases of individually identifiable information and protected health information. In these cases, the consequences range from privacy violations (including violations of both state privacy laws and federal HIPPA standards) to more serious fraud and theft (Figure 1).

On one hand, health-care data hemorrhages fuel financial identity theft. This occurs when leaked patient or employee information is used to commit traditional financial fraud. For example, using social security numbers and other identity information to apply for fraudulent loans, take-over bank accounts, or charge purchases to credit cards. On the other hand, PHI is often used by criminals to commit traditional medical fraud, which typically involves billing payers (e.g.,

Medicaid/Medicare or private health-care insurance) for treatment never rendered. The US General Accounting Office estimated that 10% of health expenditure reimbursed by Medicare is paid to fraudsters, including identity thieves and fraudulent health service providers (Bolin and Clark 2004; Lafferty 2007).

PHI can also be very valuable to criminals who are intent on committing medical identity theft. The crime of medical identity theft represents the intersection of medical fraud and identity theft (Figure 1). Like medical fraud, it involves fraudulent charges and like financial identity theft, it involves the theft of identity. It is unique in that it involves a medical identity (patient identification, insurance information, medical histories, prescriptions, test results...) that may be used to obtain medical services or prescription drugs (Ball et al. 2003). Leaked insurance information can be used to fraudulently obtain service, but unlike a credit card the spending limits are much higher—charges can quickly reach tens of thousands or even millions of dollars. And unlike financial credit, there is less monitoring and reporting. Sadly, beyond the financial losses, medical identity theft carries other personal consequences for victims as it often results in erroneous changes to medical records that are difficult and time consuming to correct. Such erroneous information could impact care quality or impede later efforts to obtain medical, life, or disability insurance.

For example, recent medical identity theft cases have involved the sale of health identities to illegal immigrants (Messmer 2008). These forms of theft are a problem impacting payers, patients, and health-care providers. Payers and providers both see financial losses from fraudulent billing. Patients are also harmed when they are billed for services they did not receive, and when erroneous information appears on their medical record.

Between 1998 and 2006, the FTC recorded complaints of over nineteen thousand cases of medical identity theft with rapid growth in the past five years. Many believe these complaints represent the tip of the growing fraud problem, with some estimates showing upwards of a quarter-million cases a year (Dixon 2006, 12-13). Currently, there is no single agency tasked with tracking, investigating, or prosecuting these crimes (Lafferty 2007) so reliable data on the extent of the problem does not exist.

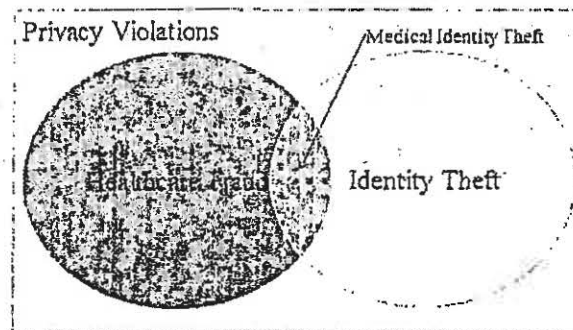


Fig. 1. Consequences of data hemorrhages.

The crime of financial identity theft is well understood with clear underlying motives. A recent FTC survey estimated that 3.7% of Americans were victims of some sort of identity theft (FTC 2007). Significant media coverage has alerted the public of the financial dangers that can arise when a thief assumes your identity. However, the dangers and associated costs of medical identity theft are less well understood and largely overlooked. Of course, PHI (including insurance policy information and government identity numbers) can be fraudulently used for financial gain at the expense of firms and individuals. However, when a medical identity is stolen and used to obtain care, it may also result in life-threatening amendments to a medical file. Any consequential inaccuracies in simple entries, such as allergy diagnoses and blood-typing results, can jeopardize patient lives. Furthermore, like financial identity theft, medical identity theft represents a growing financial burden on the private and public sectors.

Individuals from several different groups participate in the crime of medical identity theft: the uninsured, hospital employees, organized crime rings, illegal aliens, wanted criminals, and drug abusers. In many cases the theft is driven by greed, but in other cases the underlying motive is simply for the uninsured to receive medical care. Without medical insurance, these individuals are unable to obtain the expensive care that they require, such as complicated surgeries or organ transplants. However, if they assume the identity of a well insured individual, hospitals will provide full-service care. For example, Carol Ann Hutchins of Pennsylvania assumed another woman's identity after finding a lost wallet (Wereschagin 2006). With the insurance identification card inside the wallet, Hutchins was able to obtain care and medication on 40 separate occasions at medical facilities across Pennsylvania and Ohio, accumulating a total bill of \$16,000. Had it not been for the victim's careful examination of her monthly billing statement, it is likely that Hutchins would have continued to fraudulently receive care undetected. Hutchins served a 3-month jail sentence for her crime, but because of privacy laws and practices, any resulting damage done to the victim's medical record was difficult and costly to erase.

Hospital employees historically comprise the largest known group of individuals involved in traditional medical fraud. They may alter patient records, use patient data to open credit card accounts, overcharge for and falsify services rendered, create phony patients, and more. The crimes committed by hospital employees are often the largest, most intricate, and the most costly.

Take for example the case of Cleveland Clinic front desk clerk coordinator, Isis Machado who sold the medical information of more than 1,100 patients, to her cousin Fernando Ferrer, Jr., the owner of Advanced Medical Claims Inc. of Florida. Fernando then provided the information to others who used the stolen identities to file an estimated \$7.1 million in fraudulent claims (USDC 2006).

Individuals abusing prescription drugs also have a motive to commit medical identity theft. Prescription drug addicts can use stolen identities to receive multiple prescriptions at different pharmacies. Drugs obtained through this method may also be resold or traded. Roger Ly, a Nevada pharmacist allegedly filed and filled 55 false prescriptions for Oxycontin and Hydrocodone in the name of customers. Medicare and insurance paid for the drugs that Ly, allegedly, then resold or used recreationally (USA 2007). The total value of drugs sold in the underground prescription market

likely exceeds \$1 billion (Peterson 2000). Sometimes, the crimes involving prescription drugs are less serious; a Philadelphia man stole a coworker's insurance identification card to acquire a Viagra prescription, which he filled on 38 separate occasions. The plan finally backfired when the coworker he was posing as attempted to fill his own Viagra prescription and discovered that one had already been filled at another pharmacy. The cost to his company's insurance plan: over \$3,000 (PA 2006).

Wanted criminals also have a strong motive to commit medical identity theft. If they check into a hospital under their own name, they might be quickly apprehended by law enforcement. Therefore, career criminals need to design schemes to obtain care. Joe Henslik, a wanted bank robber working as an ad salesman, found it easy to obtain Joe Ryan's Social Security number as part of a routine business transaction (BW 2007). Henslik then went on to receive \$41,888 worth of medical care and surgery under Ryan's name. It took Ryan two years to discover that he had been a victim of medical identity theft. Even after discovery, he found it difficult to gain access to his medical records, since his own signature didn't match that of Henslik's forgery.

Andorice Sachs experienced a similar situation when her medical identity was used to give birth to a drug addicted baby (Reavy 2006). Sachs had lost her purse prior to the incident and had accordingly cancelled her stolen credit cards, but was unaware of the risk of medical ID theft. The baby, which was abandoned at the hospital by the mother, tested positive for illegal drug use, prompting child services to contact Sachs, who had four children of her own. Fortunately, since Sachs did not match the description of the woman who gave birth at the hospital, the problem did not escalate further. If Sachs was not able to prove her identity, she could have lost custody of her children, and been charged with child abuse. Furthermore, before the hospital became aware of the crime, the baby was issued a Social Security number in Sachs name, which could cause complications for the child later in life. Like Sachs, few individuals consider their insurance cards to be as valuable as the other items they carry in their wallet. Moreover, medical transactions appearing on a bill may not be scrutinized as closely as financial transactions with a bank or credit card.

Illegal immigrants also represent a block of individuals with a clear motive to commit medical identity theft. In the case of a severe medical emergency, they will not be refused care in most instances, but if an illegal immigrant requires expensive surgery, costly prescriptions, or other non-emergency care, they have few options. One of the most shocking and well documented cases comes from Southern California, where a Mexican resident fooled the state insurance program, Medi-Cal, into believing that he was a resident and therefore entitled to health care coverage (Hanson 1994). Mr. Hermillo Meave, was transferred to California from a Tijuana, Mexico hospital with heart problems, but told the California hospital that he was from San Diego, and provided the hospital with a Medi-Cal ID card and number. Although the circumstances surrounding Mr. Meave's arrival were suspicious, the hospital went ahead and completed a heart transplant on Mr. Meave. The total cost of the operation was an astounding one million dollars. Only after the surgery did the hospital determine that Mr. Meave actually lived and worked in Tijuana and was therefore not entitled to Medi-Cal coverage.

Perhaps emboldened by the success of Hermillo Meave, a family from Mexico sought a heart transplant for a dying relative just three months later at the very same

hospital. This time, fraud investigators were able to discover the plot before the surgery could be completed. While processing the paperwork for the patient who was checked in as Rene Garcia, Medi-Cal authorities found nine other individuals around the state, using the same name and ID number. The hospital had the family arrested and jailed for the attempted fraud, which had cost the hospital \$200,000, despite the lack of surgery. The family told investigators that they had paid \$75,000 in order to obtain the ID and set up the surgery. The trafficking of identities between Mexico and California is commonplace, but the sale of Medi-Cal identities adds a new dimension to the crime. The disparity in care between California hospitals and Mexican facilities makes the motivation to commit medical identity theft clear: falsified identification is a low-cost ticket to world-class care.

Finally, identity theft criminals often operate in crime rings, sometimes using elaborate ruses to gather the identities of hundreds of individuals. In a Houston case, criminals allegedly staged parties in needy areas offering medical deals as well as food and entertainment (USDJ 2007). At the parties, Medicaid numbers of residents were obtained and then used to bill Medicaid for alcohol and substance abuse counseling. The scheme even included fraudulent reports, written by 'certified' counselors. The fraudulent company managed to bill Medicaid for \$3.5M worth of services, of which they received \$1.8M. In this case, no medical care was actually administered and the medical identity theft was committed purely for financial reasons.

In summary, there are many reasons why individuals engage in medical identity theft, including avoiding law enforcement, obtaining care that they have no way of affording, or simply making themselves rich. Many tactics are used including first hand by physical theft, insiders, and harvesting leaked data. As we saw, PHI can be sold and resold before theft occurs—as in the case of the nine Garcias. The thief may be someone an individual knows well or it could be someone who they've never met.

For health-care providers, the first step in reducing such crime is better protection of PHI by: 1) controlling access within the enterprise to PHI; 2) securing networks and computers from direct intruders; 3) monitoring networks (internal and external) for PII and PHI transmissions and disclosures; 4) avoiding inadvertent disclosures of information. Often loose access and inadvertent disclosures are linked. When access policies allow many individuals to view, move, and store data in portable documents and spreadsheets, the risk of inadvertent disclosure increases.

3 Inadvertent Data Hemorrhages

Despite the much trumpeted enactment of the Health Insurance Portability and Accountability Act (HIPAA), data losses in the health-care sector continue at a dizzying pace. While the original legislation dates back to 1996, the privacy rules regulating the use and disclosure of medical records did not become effective until 2004. Moreover, the related security rules, which mandate computer and building safeguards to secure records, became effective in 2005. While firms and organizations have invested to protect their systems against direct intrusions and hackers, many recent data hemorrhages have come from inadvertent sources. For

example, laptops at diverse health organizations including Kaiser Permanente (Bosworth 2006), Memorial Hospital (South Bend IN) (Tokars 2008), the U.S. Department of Veterans Administration (Levitz and Hechinger 2006), and National Institutes of Health (Nakashima and Weiss 2008) were lost or stolen—in each case inadvertently disclosing personal and business information.

Organizations have mistakenly posted on the web many different types of sensitive information, from legal to medical to financial. For example, Wuesthoff Medical Center in Florida inadvertently posted names, Social Security numbers and personal medical information of more than 500 patients (WFTV 2008). Insurance and health-care information of 71,000 Georgia residents was accidentally posted on Internet for several days by Tampa-based WellCare Health Plans (Hendrick 2008).

The University of Pittsburgh Medical Center inadvertently posted patient information of nearly 80 individuals including names and medical images. In one case, a patient's radiology image was posted along with his Social Security number, insurance information, medications, and with information on previous medical screenings and procedures (Twedt, 2007). Harvard University and its pharmacy partner, PharmaCare (now part of CVS Caremark), experienced a similar embarrassment when students showed they could easily gain access to lists of prescription drugs bought by Harvard students (Russell 2005). Even technology firms like Google and AOL have suffered the embarrassment of inadvertent web posting of sensitive information (Claburn 2007, Olson 2006)—in their cases, customer information. Still other firms have seen their internal information and intellectual property appear on music file-sharing networks (DeAvila 2007), blogs, YouTube, and MySpace (Totty 2007). In each case, the result was the same: sensitive information inadvertently leaked creating embarrassment, vulnerabilities, and financial losses for the firm, its investors, and customers. In a recent data loss, Pfizer faces a class action suit from angry employees who had their personal information inadvertently disclosed on a popular music network (Vijayan 2007). In this paper we examine health-care leaks from a common, but widely misunderstood source of inadvertent disclosure: peer-to-peer file-sharing networks.

In our past research, we showed that peer-to-peer (P2P) file-sharing networks represented a significant security risk to firms operating within the banking sector (Johnson and Dynes, 2007; Johnson 2008). File sharing became popular during the late 1990s with rise of Napster. In just two years before its court-ordered closure in 2001, Napster enabled tens of millions of users to share MP3-formatted song files. Through its demise, it opened the door for many new P2P file-sharing networks such as Gnutella, FastTrack, e-donkey, and BitTorrent, with related software clients such as Limewire, KaZaA, Morpheus, eMule, and BearShare. Today P2P traffic levels are still growing with as many as ten million simultaneous users (Mennecke 2006). P2P clients allow users to place shared files in a particular folder that is open for other users to search. However, there are many ways that other confidential files become exposed to the network (see Johnson et al. 2008 for a detailed discussion). For example a user: 1) accidentally shares folders containing the information—in some cases confusing client interface designs can facilitate such accidents (Good and Kregelberg (2003)); 2) stores music and other data in the same folder that is shared—this can happen by mistake or because of poor file organization; 3) downloads

malware that, when executed, exposes files; or 4) installs sharing client software that has bugs, resulting in unintentional sharing of file directories.

While these networks are most popularly used to trade copyrighted material, such as music and video, any material can be exposed and searched for including databases, spreadsheets, Microsoft Word documents, and other common corporate file formats. The original exposure of this material over P2P networks is most likely done by accident rather than maliciously, but the impact of a single exposure can quickly balloon. After a sensitive file has been exposed, it can be copied many times by virtually anonymous P2P users, as they copy the file from one another and expose the file to more peers. Criminals are known to engage in the sale and trafficking of valuable information and data. In earlier studies using "honeypot" experiments (experiments that expose data for the purpose of observing how it is stolen), we showed how criminals steal and use both consumer data and corporate information (Johnson et al. 2008). When this leaked information happens to be private customer information, organizations are faced with costly and painful consequences resulting from fraud, customer notification, and consumer backlash.

Ironically, individuals who experience identity theft often never realize how their data was stolen. While there are many ways personal health-care data can be exposed, we will show in the next section how data hemorrhages in P2P networks represent a missing link in the "causality chain." Far worse than losing a laptop or a storage device with patient data (Robenstein 2008), inadvertent disclosures on P2P networks allow many criminals access to the information, each with different levels of sophistication and ability to exploit the information. And unlike an inadvertent web posting, the disclosures are far less likely to be noticed and corrected (since few organizations monitor P2P and the networks are constantly changing making a file intermittently available to a subset of users). Clearly, such hemorrhages violate the privacy and security rules of HIPAA, which call for health-care organizations to ensure implementation of administrative safeguards (in the form of technical safeguards and policies, personnel and physical safeguards) to monitor and control intra and inter-organizational information access.

4 Research Method and Analysis

To explore the vulnerability and threat of medical information leakage, we examined health-care data disclosures and search activity in peer-to-peer file sharing networks. To collect a sample of leaked data, we initially focused on Fortune Magazine's list of the top ten publically traded health-care firms (Fortune Magazine (Useem 2007)). Together those firms represented nearly \$70B in US health-care spending (Figure 2).

To gather relevant files, we developed a digital footprint for each health-care institution. A digital footprint represents key terms that are related to the firm—for example names of the affiliated hospitals, clinics, key brands, etc. Searching the internet with Google or P2P networks using those terms will often find files related to those institutions. With the help of Tiversa Inc., we searched P2P networks using our digital signature over a 2-week period (in January, 2008) and randomly gathered a sample of shared files related to health care and these institutions. Tiversa's servers

and software allowed us to sample in the four most popular networks (each of which supports the most popular clients) including Gnutella (e.g., Limewire, BearShare), FastTrack (e.g., KaZaA, Grokster), Aries (Aries Galaxy), and e-donkey (e.g., eMule, EDonkey2K). Files containing any one or combination of these terms in our digital footprint were captured. We focused on files from the Microsoft Office Suite (Word, Powerpoint, Excel, and Access). Of course, increasing the number of terms included in the digital footprint increases the number file matches found, but also increases false positives—files captured that have nothing to do with the institution in question. Given the large number of hospitals within these ten organizations (more than 500), our goal was to gather a sample of files to characterize the ongoing data hemorrhage. Since users randomly join P2P networks to get and share media (and then depart), the network is constantly changing. By randomly sampling over a 14-day period, we collected 3,328 files for further (manual) analysis.

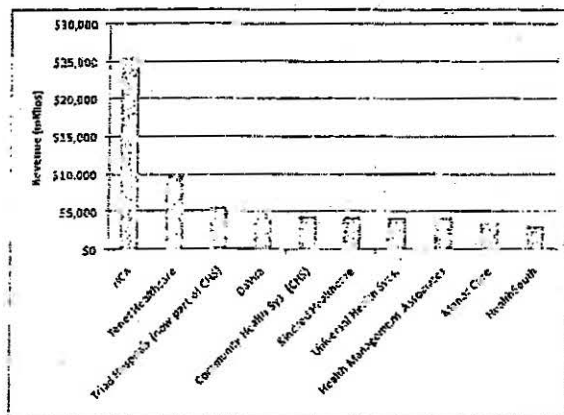


Fig. 2. Revenue of the top ten US health-care firms (Useem 2007).

Of 3,328 documents in our sample, 50.3% could be immediately identified as duplicate copies of the same file (same hash) that had spread or were on multiple IP addresses, leaving us with 1,654 documents to categorize. While duplicate files were not downloaded from the same IP address, duplicate files were collected when a target file had spread to multiple sharing clients. They were also collected from users who joined the network at different IP addresses (what we call an IP shift). Through a manual analysis of the remaining 1,654 files, we found that 71% were not relevant to health care or the organizations under consideration and were downloaded because our search terms overlapped with other subject matter. This was the result of the size and quality of our digital footprint. By casting a large net, we found more files but also many that were not related to the health-care sector. Of the remaining 475 documents, 86 were manually evaluated as duplicate files. With this cross section of

data associated with the health-care organizations, we categorized each file evaluating the dangers associated with it. Figure 3 shows a categorization of the 389 unique, relevant files.

The most common type of files found were newspaper and journal articles, followed by documents associated with students studying medicine. This should not come as a surprise as many P2P users are students. Interestingly, we found entire medical texts being shared. We also found many documents dealing directly with medical issues, such as billings, letters to hospitals, and insurance claims. Many of these documents were leaked by patients themselves. For example, we found several patient-generated spreadsheets containing details of medical treatments and costs—likely for tax purposes. Other documents discovered included hospital brochures and flyers, which were intended for public consumption. Finally there were job listings, cover letters, and résumés, all likely saved on computers of job-seekers. The lack interest in sharing these files for a typical P2P user makes it readily apparent that they were likely shared by mistake. However, all of the files weren't so innocuous. After categorizing the files, we found that about 5% of the files recovered by our loosely tuned search were sensitive or could be used to commit medical or financial identity theft.

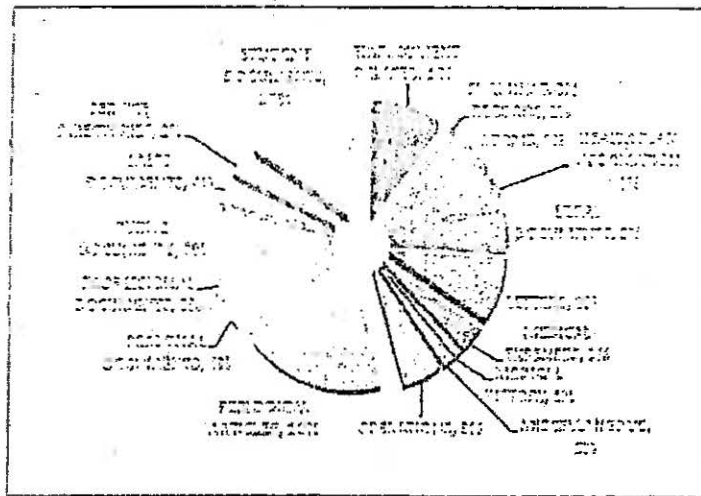


Fig. 3. Summary of unique relevant files.

The set of dangerous documents discovered contained several files that would facilitate medical identity theft. One such document was a government application for employment asking for detailed background information. The document contained the individual's Social Security number, full name, date of birth, place of

birth, mother's maiden name, history of residence and acquaintances, schooling history, and employment history (the individual had worked at one of the hospitals under study). Despite the document's three-page forward highlighting the privacy act measures undertaken by the government to protect the information in the document, and the secure Data Hash code stamped at the bottom of every page along with the bolded text 'PRIVACY ACT INFORMATION', this document somehow ended up on to a P2P network.

More disturbing, we found a hospital-generated spreadsheet of personally identifiable information on recently-hired employees including Social Security numbers, contact information, job category etc. Another particularly sensitive document was an Acrobat form used for creating patient prescriptions. The scanned blank document was signed by a physician and allowed for anyone to fill in the patient's name and prescription information. This document could be used for medical fraud by prescription drug dealers and abusers. Additionally, the doctor's own personal information was included in the document, giving criminals the opportunity to forge other documents in his name. Finally, another example we found was a young individual's medical card. This person was suffering from various ailments and was required to keep a card detailing his prescription information. The card included his doctor's name, parent's names, address, and other personal information. A person with a copy of this identification card could potentially pose as the patient and attempt to procure prescription drugs. All of these dangerous files were found with a relatively simple sample of files published for anyone to find.

As a second stage of our analysis, we then moved from sampling with a large net to more specific and intentional searches. Using information from the first sampling, we examined shared files on hosts where we had found other dangerous data. One of the features enabled by LimeWire and other sharing clients is the ability to examine all the shared files of a particular user (sometimes called "browse host"). Over the next six months, we periodically examined hosts that appeared promising for shared files.

Using this approach, we uncovered far more disturbing files. For a medical testing laboratory, we found a 1,718-page document containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients. Figure 4 shows a redacted excerpt of just a single page of the insurance aging report containing patient name, Social Security number, date of birth, insurer, group number, and identification number. All together, almost 9,000 patient identities were exposed in a single file, easily downloaded from a P2P network.

For a hospital system, we found two spreadsheet databases that contained detailed information on over 20,000 patients including Social Security numbers, contact details, and insurance information. Up to 82 fields of information (see Figure 5) were recorded for each patient—representing the contents of the popular HCFA form. In this case, the hemorrhage came from an outsourced collection agency working for the hospital. However, besides the patients and hospital system, many other

1. FAFA billNumber	28. dtscargeDate	55. firstInsuranceName
2. providerName	29. patientAedRecNo	56. firstInsuranceAddressLine1
3. providerAddressLine1	30. patientMaritalStatus	57. firstInsuranceCity
4. providerCityStateZip	31. guarantorFirstName	58. firstInsuranceState
5. providerPhoneNumber	32. guarantorLastName	59. firstInsuranceZipCode
6. providerFederalTaxId	33. guarantorSSN	60. firstPolicyNumber
7. patientFirstName	34. guarantorPhone	61. firstAuthorizationNumber
8. patientMiddleInitial	35. guarantorAddressLine1	62. firstGroupName
9. patientLastName	36. guarantorAddressLine2	63. firstGroupNumber
10. patientSSN	37. guarantorCity	64. firstInsuredRelationship
11. patientPhone	38. guarantorState	65. firstDateEligible
12. patientAddressLine1	39. guarantorZipCode	66. firstDateThru
13. patientAddressLine2	40. guarantorBirthDate	67. secondInsuranceName
14. patientCity	41. guarantorEmployerName	68. secondInsuranceAddressLine1
15. patientState	42. guarantorEmployerAddressLine1	69. secondInsuranceCity
16. patientZipCode	43. guarantorEmployerAddressLine2	70. secondInsuranceState
17. patientSex	44. guarantorEmployerCity	71. secondInsuranceZipCode
18. patientBirthDate	45. guarantorEmployerState	72. secondPolicyNumber
19. patientEmployerName	46. guarantorEmployerZipCode	73. secondGroupName
20. patientEmployerAddressLine1	47. guarantorEmployerPhone	74. secondGroupNumber
21. patientEmployerAddressLine2	48. guarantorRelationship	75. secondInsuredRelationship
22. patientEmployerCity	49. totalCharges	76. secondDateEligible
23. patientEmployerState	50. amountBalance	77. secondDateThru
24. patientEmployerZipCode	51. totalPayments	78. primaryDiagnosisCode
25. patientEmployerPhone	52. totalAdjustments	79. attendingPhysician
26. caseType	53. accidentCode	80. attendingPhysicianUPIN
27. admissionDate	54. accidentDate	81. lastPaymentDate
		82. providerShortName

Fig. 5. File contents for over 20,000 patients in on inadvertent disclosure.

organizations were comprised. The data disclosed in this file well-illustrates the complexity of US health care with many different constituencies represented, including 4 major hospitals, 335 different insurance carriers acting on behalf of 4,029 patient employers, and 266 different treating doctors (Figure 6). Each of these constituents was exposed in this disclosure. Of course, the exposure of sensitive patient health-information may be the most alarming to citizens. Figure 7 shows one very small section of the spreadsheet (just three columns of 82) for a few patients (of the nearly 20,000). Note that the diagnosis code (IDC code) is included for each patient. For example, code 34 is streptococcal sore throat; 42 is AIDS; 151.9 is malignant neoplasm of stomach (cancer); 29 is alcohol-induced mental disorders; and 340 is multiple sclerosis. In total the file contained records on 201 patients with different forms of mental illness, 326 with cancers, 4 with AIDS, and thousands with other serious and less serious diagnoses.

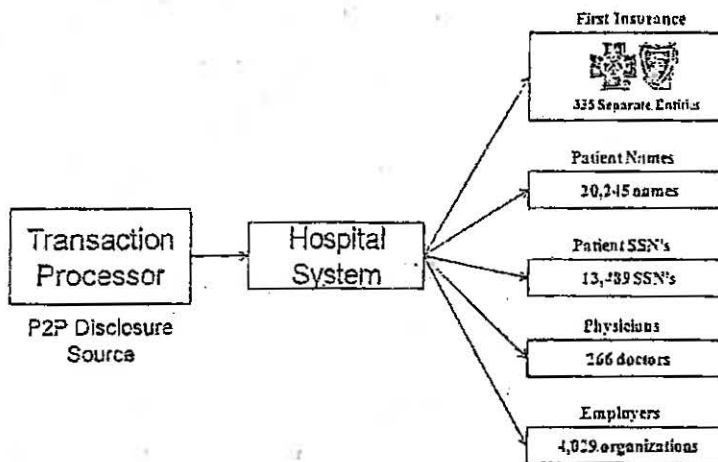


Fig. 6. Hemorrhage exposed a large array of health-care constituents.

CA	CB	CC
primaryDiagnosisCode	attendingPhysician	attendingPhysicianUPN
8 45		
34		
34		
34		
42		
151 9		
152 1		
291		
291 81		
292		
292 62		
340		
340		
700 25		
700 38		
700 4		
700 5		
700 6		
700 79		
700 79		
700 99		
705		
751		
803		
170 0		
170 12		
170 13		

Fig. 7. Disclosures expose extremely personal diagnosis information. A very small section of a spreadsheet for a few (of over 20,000) patients showing ICD diagnosis codes (see <http://www.ems.hhs.gov/ICD9ProviderDiagnosticCodes/> or <http://www.icd9data.com/>). Personally Identifiable Information has not been included in the illustration to protect the identities of the patients and physicians.

For a mental health center, we found patient psychiatric evaluations. All would be considered extremely personal and some were disturbing. We found similar clinical evaluations leaking from Alabama to Nebraska to California.

Of course, these are just few of many files we uncovered. For a group of anesthesiologists, we found over 350MB of data comprising patient billing reports. For a drug and alcohol rehab center, we found similar billing information. From an AIDs clinic we found a spreadsheet with 232 clients including address, Social Security number, and date of birth. And the list goes on. It is important to note that all of these files were found without extraordinary effort and certainly far less effort than criminals might be economically incented to undertake.

With the vulnerability well established, we also investigated the search activity in P2P networks to see if users were looking for health-care data hemorrhages. Again, using our simple digital signature we captured a sample of user-issued searches along with our files. Figure 8 lists a sample of these searches and clearly shows that users are searching for very specific health-care related data in P2P networks.

care office rbc health
 medicine mental health cmc of
 hospital records
 mental hospitals
 hospital
 hospital letterhead
 hospital records
 niagara hospital
 american medical
 conroy medical ups prostate
 data entry medical billing fax
 deal medical insurance my
 details of medical insurance
 herdaaw r medical imaging
 info medical
 medical
 medical claims
 medical exam
 medical history
 medical passwords
 medical permission
 medical records certificate on
 medical release
 medical secretary cover letter
 medicine medical passwords
 submission for medical
 authorization for medical of b
 authorization form medical of
 authorization form medical
 basic medical forms
 basic medical laboratory techn
 berry medical jack insurance
 billing medical
 billy conroy medical
 checkup
 billy conroy medical check
 canadian medical
 canadian medical
 canadian medical association
 canadian medical law
 caufield general medical
 cbt correct medical expenses
 certibat medical
 certibat medical
 certibat medical
 charles medical costs
 charles medical costs on the
 ch's medical exam
 chid medical exams
 chid medical release form
 cigna medical dr
 cigna medications
 classified medical records
 complete medical exam
 comprehensive medical
 computer medical
 computer medical
 computer medical billing
 tu
 computers in the medical office
 computers medical doctors
 conroy medical check bily
 conroy medical usa
 billing medical august
 dear medical assurance my
 dear medical insurance my
 dear medical my assurance
 details of medical insurance
 dental medical cross coding
 detective medical
 digital (pa. medical trans
 distribute medical
 doctor - medical checkup
 doctor takes medical by exam
 doctor medical exam
 Doctors medical billing
 doctors office medical exam
 doctors order medical doctor
 doctors orders medical
 doug medical bill
 doug stanhope medical pms
 d'Am's medical software 3.9
 electronic medical
 electronic medical record
 electronic medical record vax
 electronic medical record.pdf
 electronic medical records
 electronic medical systems
 electronics & bio medical
 emt medical software
 forms medical
 forms medical activity form
 forms medical office
 ge medical
 ge medical systems
 medical coding and billing
 medical coding exam
 letter for medical bills
 letter for medical bills dr
 letter for medical bills etmc
 letter re medical bills 102h
 lr c'snt medical report
 lr hyn mahmah medical
 lr medical bodyfile
 lr medical system portland
 lr medical msc portland
 lr orange medical head center
 lr to vafay medical
 lytec medical billing
 medical investigation
 medical journals pass and
 medical list
 medical abuse records
 medical abuse records
 medical abuse records
 medical applications
 medical authorization form
 medical authorization form
 medical benefits
 medical benefits plan chca
 medical billing
 medical billing
 medical bill
 medical bill resume
 medical billing software
 medical billing windows

Fig. 8. Selection of User-Issued searches that contain the word medical or hospital

5 Conclusion

Data hemorrhages from the health-care sector are clearly a significant threat to providers, payers, and patients. The inadvertent disclosures we found and documented in this report point to the larger problem facing the industry. Clearly, such hemorrhages may fuel many types of crime. While medical fraud has long been a significant problem, the crime of medical identity theft is still in its infancy. Today, many of the well-documented crimes appear to be committed out of medical need. However, with the growing opportunity to commit more significant crimes involving large financial rewards, more and more advanced schemes and methods, such as P2P-fueled identity theft, will likely develop. For criminals to profit, they don't need to "steal" an identity, but only to borrow it for a few days, while they bill the insurer thousands of dollars for fabricated medical bills. This combination of medical fraud along with identity theft adds a valuable page to the playbook of thieves looking for easy targets. Stopping the supply of digital identities is one key to halting this type of illegal activity.

The Health Insurance Privacy Accountability Act (HIPAA) was created to protect patients from having sensitive medical information from becoming public or used against them. However, some of the provisions of the act make medical identity theft more difficult to track, identify, and correct. Under HIPAA, when a patient's medical record has been altered by someone else using their ID, the process to correct the record is difficult for the patient. The erroneous information in the medical file may remain for years. Also due to the intricacies of HIPAA, people who have been victims of medical identity theft may find it difficult to even know what has been changed or added to their record. Since the thief's medical information is contained within the victim's file, it is given the same privacy protections as anyone under the act. Without the ability to remove erroneous information, or figure out the changes contained in a medical record, repairing the damages of medical identity theft can be a very taxing process.

However, HIPAA is also a positive force in the fight against identity theft. Institutions have been fined and required to implement detailed corrective action plans to address inadvertent disclosures of identifiable electronic patient information (HHS 2008). In the case of Isis Machado mentioned earlier, she was charged and fined under HIPAA for disclosing individually identifiable medical records. HIPAA contains rules and punishments for offending medical professionals, which are historically the largest group of health-care fraud perpetrators. This protection of patient identities does discourage inappropriate uses of medical information and reduces the chance of hemorrhages. Nevertheless, HIPAA can do little to stop patients from disclosing their medical identities voluntarily to individuals posing as health care providers, or poorly managing their own computerized documents.

Tighter controls on patient information are a good start, but consumers still need to be educated of the dangers of lost health-care information and how to secure their information on personal computers. Hospitals and others concerned with medical identity theft have begun to undertake measures in order to curb medical identity theft. One of the simplest and most effective measures put in place by hospitals is to request photo identification for admittance to the hospital. In many cases, when a request for photo identification is made, the individual will give up on obtaining care and simply leave the hospital, never to return again. Of course, this measure will likely lose its efficacy in time as criminals become aware of the change in policy. Once a few personal identifiers have been acquired, such as date of birth and Social Security number, a criminal can obtain seemingly valid photo-ID. In the future, insurance companies may need to begin issuing their own tamper-proof photo identification to help stop medical identity theft.

Finally, health-care providers and insurers must enact better monitoring and information controls to detect and stop leaks. Information access within many health-care systems is lax. Coupled with the portability of data, inadvertent disclosures are inevitable. Better control over information access governance (Zhao and Johnson 2008) is an important step in reducing the hemorrhages documented in this report.

References

1. Ball, E., Chadwick, D.W., Mundy, D. (2003), "Patient Privacy in Electronic Prescription Transfer," *IEEE Security & Privacy*, March/April, 77 - 80.
2. Bolin, J.N., Clark, L.S. (2004), "Avoiding Charges of Fraud and Abuse: Developing and Implementing an Effective Compliance Program," *JONA* (34:12), 546-550.
3. Bosworth, M.H. (2006), "Kaiser Permanente Laptop Stolen: Personal Data on 38,000 Members Missing," *Consumer Affairs*, Nov 29, http://www.consumeraffairs.com/news04/2006/11/kaiser_laptop.html
4. BW (2007), "Diagnosis: Identity Theft," *Business Week*, January 8, 2007.
5. Claburn, T. (2007), "Minor Google Security Lapse Obscures Ongoing Online Data Risk," *Information Week*, January 22.
6. De Avila, J. (2007), "The Hidden Risk of File-Sharing," *Wall Street Journal*, Nov. 7, D1.
7. Dixon, P. (2006), "Medical Identity Theft: The Information Crime that Can Kill You," *The World Privacy Forum*.
8. FBI (2007), "2006 Financial Crime Report" Federal Bureau of Investigation. [Online] 02 28, 2007. [Cited: 02 04, 2008.] http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm.
9. FTC (2007), "2006 Identity Theft Report," Federal Trade Commission, November, 2007, last accessed on June 18, 2008, <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>
10. Good N.S., and A. Krekelberg (2003) "Usability and privacy: a study of Kazan P2P file-sharing," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, April 05-10.
11. Hanson, G (1994), "Illegal Aliens Bilk Sick U.S. system," *Insight on the News*, April 18, 1994.
12. Hendrick, B. (2008), "Insurance records of 71,000 Ga. families made public," *Atlanta Journal-Constitution*, April 08. http://www.ajc.com/metro/content/metro/stories/2008/04/08/08breach_6-09.html
13. HHS (2008), "HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information," U.S. Department of Health & Human Services, News Release, July 17, <http://www.hhs.gov/news/press/2008pres/07/20080717a.html>
14. Johnson, M. E. and S. Dynes (2007), "Inadvertent Disclosure: Information Leaks in the Extended Enterprise," *Proceedings of the Sixth Workshop on the Economics of Information Security*, Carnegie Mellon University, June 7-8.
15. Johnson, M. E. (2008), "Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain," *Journal of Management Information Systems*, Vol. 25, No. 2, 97-123.
16. Johnson, M. E., D. McGuire, and N. D. Willey (2008), "The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users," *Proceedings of HICSS-41, International Conference on System Sciences*, IEEE Computer Society, Jan 7-10, Hawaii.
17. Johnson, M. E., McGuire, D., and N. D. Willey (2009), "Why File Sharing Networks Are Dangerous," *Communications of the ACM*, 52, 2, 134-138.
18. Lafferty, L. (2007), "Medical Identity Theft: The Future Threat of Health Care Fraud Is Now," *Journal of Health Care Compliance*, Jan/Feb, 9, 1, 11-20.
19. Levitz, J. and J. Hechinger (2006), "Laptops Prove Weakest Link in Data Security," *Wall Street Journal*, March 26.
20. Mennecke, T. (2006), "Slyck News - P2P Population Continues Climb," June 14, <http://www.slyck.com/news.php?story=1220>.

21. Messmer, E. (2008), "Health Care Organizations See Cyberattacks as Growing Threat," *Network World*, February 28.
22. Musco, T. D. and K. H. Fyffe (1999), "Health Insurers' Anti-fraud Programs," Washington D.C. Health Insurance Association of America.
23. Nakashima, E. and R. Weiss (2008), "Patients' Data on Stolen Laptop," *Washington Post*, March 24, A1.
24. Olson, P. (2006), "AOL Shoots Itself in the Foot," *Forbes*, August 8.
25. PA (2006), "Pennsylvania Attorney General. Attorney General's Insurance Fraud Section charges former SEPTA employee with using co-worker's ID to obtain Viagra." *Harrisburg: s.n.*, July 6, 2006.
26. Peterson, M. (2000), "When Good Drugs Go Gray: Booming Underground Market Raises Safety Concerns," *The New York Times*, 12 14, 2000, p. 1.
27. Reavy, P. (2006), "What Baby? ID victim gets a jolt," *Deseret News (Salt Lake City)*, May 2, 2006.
28. Robenstein, S. (2008), "Are Your Medical Records at Risk?" *Wall Street Journal*.
29. Russell, J. (2005), "Harvard fixing data security breaches: Loophole allowed viewing student prescription orders" *Boston Globe*, January 22.
30. Tokars, L. (2008), "Memorial Hospital loses laptop containing sensitive employee data," *WSBT*, Feb 7, <http://www.wsbj.com/news/local/15408791.html>
31. Totty, M. (2007), "Security: How to Protect Your Private Information," *Wall Street Journal*, January 29. R1.
32. Twedt, S. (2007), "UPMC patients' personal data left on Web," *Pittsburgh Post-Gazette*, April 12.
33. USDC (2006), "United States of America vs. Fernando Ferrer, Jr. and Isis Machado." 06-60261, s.l., United States District Court Southern District of Florida, September 7, 2006.
34. USDJ (2007), "US Department of Justice. Six Indicted for Health Care Fraud Scheme in Southeast Texas," *Houston TX: s.n.*, 2007. Press Release.
35. USA (2007), "United States Attorney, District of Nevada. "Las Vegas Pharmacist Charged with Health Care Fraud and Unlawful Distribution of Controlled Substances," *Las Vegas, United States Department of Justice*, 2 23, 2007.
36. Useem, J. (2007), "Fortune 500: The Big Get Bigger," *Fortune Magazine*, 155, 8, April 30. 81. *Wall Street Journal*, March 26.
37. Vijayan, J. (2007), "Personal data on 17,000 Pfizer employees exposed; P2P app blamed." *Computer World*
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=902449>
38. Wereschagin, Mike (2006), "Medical ID Theft Leads to Lengthy Recovery." *Pittsburgh Tribune-Review*, 10 24, 2006.
39. WFTV (2008), "Medical Center Patient Records Posted On Internet," August 14, <http://www.wftv.com/news/17188045/detail.html?tab=orlc>
40. Zhao, X. and M. E. Johnson (2008), "Information Governance: Flexibility and Control through Escalation and Incentives," *Proceedings of the Seventh Workshop on the Economics of Information Security*, Dartmouth College, June 26-27.

Exhibit C

- B) To present testimony by deposition and/or investigational hearing transcript, affidavit, declaration, or orally by live witness, from persons listed below and any other person that Respondent identifies as a potential witness in this action;
- C) To amend this Final Proposed Witness List to be consistent with the Court's ruling on any pending motions, including any motions *in limine* filed in this matter;
- D) To question the persons listed below about any topics that are the subjects of testimony by witnesses to be called by Respondent;
- E) Not to present testimony by deposition and/or investigational hearing transcript, affidavit, declaration, or orally by live witness, from any of the persons listed below;
- F) To question any person listed below about any other topics that the person testified about at his or her deposition or investigational hearing, or about any matter that is discussed in any documents to which the person had access and which are designated as exhibits by either party or which have been produced since the person's deposition was taken;
- G) To present testimony by deposition and/or investigational hearing transcript, affidavit, declaration, or orally by live witness, from any persons, regardless whether they are listed below, to rebut the testimony of witnesses proffered by Respondent;
- H) For any individual listed below as being associated with a corporation, government agency, or other non-party entity, to substitute a witness designated by the associated non-party entity; and

- D) To supplement this Final Proposed Witness List in light of Respondent's Final Proposed Witness List and Exhibit List, or as circumstances may warrant.

Subject to these reservations of rights, Complaint Counsel's Final Proposed Witness List is as follows:

Current and Former LabMD Employees

1. John Boyle, former LabMD Vice President of Operations, in his individual capacity

Mr. Boyle will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's information-technology ("IT") related expenditures; management of LabMD's compliance program; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

2. John Boyle, former LabMD Vice President of Operations, LabMD designee

Mr. Boyle will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; management of LabMD's compliance program; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in the investigational hearing of LabMD; any documents introduced into evidence by

Respondent or Complaint Counsel as to which LabMD has knowledge; or any other matters as to which LabMD has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

3. Brandon Bradley, former LabMD IT employee

Mr. Bradley will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

4. Sandra Brown, former LabMD finance or billing employee

Ms. Brown will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

5. Matt Bureau, former LabMD IT employee

Mr. Bureau will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training;

the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

6. Michael Daugherty, LabMD President and Chief Executive Officer, in his individual capacity

Mr. Daugherty will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition or investigational hearing; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

7. Michael Daugherty, LabMD President and Chief Executive Officer, LabMD designee

Mr. Daugherty will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into

evidence by Respondent or Complaint Counsel as to which LabMD has knowledge; or any other matters as to which LabMD has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

8. Jeremy Dooley, former LabMD Communications Coordinator and IT employee
Mr. Dooley will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

9. Kim Gardner, former LabMD Executive Assistant

Ms. Gardner will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; information relating to the wind down of LabMD's business operations and the corresponding relocation of LabMD's business premises; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

10. Karalyn Garrett, former LabMD finance or billing employee

Ms. Garrett will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

11. Patricia Gilbreth, former LabMD finance or billing employee

Ms. Gilbreth will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

12. Nicotra Harris, former LabMD finance or billing employee

Ms. Harris will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues

addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

13. Patrick Howard, former LabMD IT employee

Mr. Howard will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

14. Lawrence Hudson, former LabMD sales employee

Ms. Hudson will testify about LabMD's computer networks, including, but not limited to remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

15. Robert Hyer, former LabMD IT Manager and former LabMD contractor

Mr. Hyer will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

16. Curt Kaloustian, former LabMD IT employee

Mr. Kaloustian will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his investigational hearing; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

17. Eric Knox, former LabMD sales employee

Mr. Knox will testify about LabMD's computer networks, including, but not limited to remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or

Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

18. Chris Maire, former LabMD IT employee

Mr. Maire will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

19. Jeff Martin, former LabMD IT employee and former LabMD contractor

Mr. Martin will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

20. Jennifer Parr, former LabMD IT employee

Ms. Parr will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the

personal information to which she and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

21. Alison Simmons, former LabMD IT employee

Ms. Simmons will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition or investigational hearing; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

22. LabMD, designee(s) to be determined

The LabMD designee(s) will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in its deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which LabMD has knowledge; or any other matters as to which LabMD has knowledge that are

relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. The designee(s) will also testify about any other topics listed in the deposition notice that was issued by Complaint Counsel to LabMD in this action.

Current and Former Clients of LabMD

23. Letonya Randolph, Midtown Urology, PC ("Midtown Urology") employee, Midtown Urology designee

Ms. Randolph will testify about Midtown Urology's relationship and communications with LabMD; computer hardware and software provided to Midtown Urology by LabMD, and the maintenance thereof; the transmission of personal information between Midtown Urology and LabMD; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which Midtown Urology has knowledge; or any other matters as to which Midtown Urology has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. She will also testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to Midtown Urology in this action, and the admissibility of those documents into evidence in the hearing in this action.

24. Barbara Goldsmith, Midtown Urology, PC ("Midtown Urology") employee

Ms. Goldsmith will testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to Midtown Urology in this action, and the admissibility of those documents into evidence in the hearing in this action.

25. Jerry Maxey, Southeast Urology Network ("S.U.N.") employee, S.U.N. designee

Mr. Maxey will testify about S.U.N.'s relationship and communications with LabMD; computer hardware and software provided to S.U.N. by LabMD, and the maintenance thereof; the transmission of personal information between S.U.N. and LabMD; any other

issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which S.U.N. has knowledge; or any other matters as to which S.U.N. has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. He will also testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to S.U.N. in this action, and the admissibility of those documents into evidence in the hearing in this action.

Contractors and Other Individuals and Entities
Who Have Provided Services or Equipment to LabMD

26. Lou Carmichael, former LabMD consultant

Ms. Carmichael will testify about LabMD's security policies and practices, compliance program, and employee training; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

27. Hamish Davidson, President of ProviDyn, Inc.

Mr. Davidson will testify about facts related to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to ProviDyn, Inc. in this action, and the admissibility of those documents into evidence in the hearing in this action.

28. Allen Truett, former Chief Executive Officer of Automated PC Technologies, Inc.

Mr. Truett will testify about LabMD's computer networks, including, but not limited to, remote access thereto; the products and/or services that he and his company, Automated PC Technologies, Inc., provided to LabMD, including, but not limited to the security features

of those products and/or services; the communications between LabMD and Mr. Truett or Automated PC Technologies, Inc.; the facts underlying and set forth in the affidavit that Mr. Truett executed on May 20, 2011, which LabMD submitted to Commission staff during the Part II investigation; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

29. Peter Sandrev, Broadvox employee, Cypress Communications, LLC ("Cypress") designee

Mr. Sandrev will testify about LabMD's computer networks, including, but not limited to the products and/or services that Cypress has provided to LabMD, including but not limited to any security features of those products and/or services; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which Cypress has knowledge; or any other matters as to which Cypress has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. He will also testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to Cypress in this action, and the admissibility of those documents into evidence in the hearing in this action.

Other Individuals and Entities

30. Robert Boback, Chief Executive Officer of Tiversa Holding Corporation ("Tiversa"), Tiversa designee

Mr. Boback will testify about Tiversa's understanding and use of peer-to-peer file sharing applications and networks; Tiversa's communications with LabMD; facts relating to

how Tiversa obtained multiple copies of the “P2P insurance aging file” referenced in Paragraph 17 of the Complaint and the different IP addresses from which Tiversa obtained copies of that file; other facts relating to the security incident alleged in Paragraphs 17-20 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which Tiversa has knowledge; or any other matters as to which Tiversa has knowledge that are relevant to the allegations of the Complaint, Respondent’s affirmative defenses, or the proposed relief. Mr. Boback will also testify about facts relating to the documents produced in response to Complaint Counsel’s subpoena *duces tecum* to Tiversa in this action, and the admissibility of those documents into evidence in the hearing in this action.

31. Erick Garcia

Mr. Garcia will testify about facts relating to the security incident alleged in Paragraph 21 of the Complaint.

32. Karina Jestes, Detective, Sacramento, CA Police Department

Detective Jestes will testify about facts relating to the security incident alleged in Paragraph 21 of the Complaint, including but not limited to, facts relating to her investigation of the conduct underlying the pleas of no contest to California charges of identity theft entered by Erick Garcia and Josie Martinez Maldonado; her training and experience as it relates to identity theft; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent’s affirmative defenses, or the proposed relief. Detective Jestes will also testify about facts relating to the documents produced in response

to Complaint Counsel's subpoena *duces tecum* to the Custodian of Records of the Sacramento, CA Police Department in this action, and the admissibility of those documents into evidence in the hearing in this action.

33. M. Eric Johnson, Dean of Owen Graduate School of Management, Vanderbilt University

Dean Johnson will testify about facts related to his study entitled "Data Hemorrhages in the Health-Care Sector," including his research methodology and findings; the "P2P insurance aging file" referenced in Paragraph 17 of the Complaint; facts relating to the security incident alleged in Paragraphs 17-20 of the Complaint; peer-to-peer file sharing applications and networks and the consequences of inadvertent disclosures of consumers' personal information; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

34. Roger Jones, Records Section Supervisor, Sandy Springs, GA Police Department

Mr. Jones will testify about facts related to the admissibility of documents that were produced in response to Complaint Counsel's subpoena *duces tecum* to the Sandy Springs, GA Police Department into evidence in the hearing in this action.

35. David Lapidès, Detective, Sandy Springs, GA Police Department

Detective Lapidès will testify about his communications with LabMD and other facts relating to the security incident alleged in Paragraph 21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which he has knowledge; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative

defenses, or the proposed relief. Detective Lapides will also testify about facts relating to documents that were produced in response to Complaint Counsel's subpoena *duces tecum* to the Sandy Springs, GA Police Department in this action, and the admissibility of those documents into evidence in the hearing in this action.

36. Susan McAndrew, Deputy Director for Health Information Privacy, Office for Civil Rights, or other designee, U.S. Department of Health and Human Services ("HHS")

Ms. McAndrew, or another designee of HHS, will testify about the existence or non-existence of any evaluations by HHS of LabMD's compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the regulations promulgated under HIPAA and HITECH.

37. Jonn Perez, Trend Micro Inc. employee

Mr. Perez will testify about facts related to the admissibility of documents that were produced in response to Complaint Counsel's subpoena *duces tecum* to Trend Micro Inc.

38. Euly Ramirez, Supervisor, Sacramento, CA Police Department

Ms. Ramirez will testify about facts related to the admissibility of documents produced in response to Complaint Counsel's subpoena *duces tecum* to the Custodian of Records of the Sacramento, CA Police Department into evidence in the hearing in this action.

39. Matt Wells, Trend Micro Inc. employee

Mr. Wells will testify about facts related to the admissibility of documents that were produced in response to Complaint Counsel's subpoena *duces tecum* to Trend Micro Inc.

40. Kevin Wilmer, Investigator, Federal Trade Commission, Bureau of Consumer Protection, Division of Privacy and Identity Protection

Mr. Wilmer will testify about the process used to identify the individuals listed in Appendix A (designated as “CONFIDENTIAL”) to Complaint Counsel’s Initial Disclosures as “Individuals Associated with 9-Digit Numbers Listed in the Day Sheets Referenced in Paragraph 21 of the Complaint Whose Names Are Not Listed in Those Day Sheets,” which has been produced at FTC-010907.

41. Nathaniel Wood, Assistant Director, Federal Trade Commission, Bureau of Consumer Protection, Division of Consumer and Business Education

Mr. Wood will testify about facts related to the admissibility of certain documents produced as part of Complaint Counsel’s Initial Disclosures into evidence in the hearing in this action.

Expert Witnesses

42. Raquel Hill, PhD

Professor Hill is an Associate Professor at Indiana University, School of Informatics and Computing, and a Visiting Scholar at Harvard University’s School of Engineering and Applied Science, Center for Research on Computation and Society. Her research focuses on trust and security for distributed computing environments and privacy of medical related data. She received both her Bachelor of Science and Master of Science in Computer Science from the Georgia Institute of Technology. She received her PhD in Computer Science from Harvard University in 2002.

Professor Hill will testify, from her perspective as an expert in computer security, data privacy, and networking systems, regarding whether LabMD: (1) failed to provide reasonable and appropriate security for consumers’ personal information within its computer

network and (2) could have corrected any such security failures at relatively low cost using readily available security measures. Her testimony is based on transcripts and exhibits from investigational hearings and depositions of Respondent, its current and former employees, and third parties; correspondence and documents submitted by Respondent 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.

43. Rick Kam, CIPP/US

Mr. Kam is a Certified Information Privacy Professional (CIPP/US), and is the President and Co-Founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. In this role, Mr. Kam has had the opportunity to work on data breach incidents as part of ID Experts' incident response team. ID Experts has managed hundreds of data breach incidents, protecting millions of affected individuals and restoring the identities of thousands of identity theft victims. Within the healthcare industry, Mr. Kam has worked with organizations ranging in size from individual providers and small clinics to large hospital systems and health insurance companies. Mr. Kam also serves in leadership roles of organizations addressing identity theft, medical identity theft, and data breach risk and remediation, and he presents regularly at conferences and frequently publishes pieces regarding these and other subjects.

Mr. Kam will testify, from his perspective as an expert in identifying and remediating the consequences of identity theft and medical identity theft, about the risk of harm, particularly from medical identity theft, to consumers whose sensitive personal information LabMD disclosed without authorization. Mr. Kam will also testify about consequences of

the risk of unauthorized disclosure caused by LabMD's failure to provide reasonable and appropriate security for consumers' personal information maintained on its computer network.

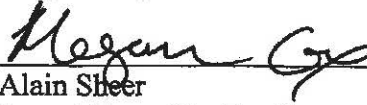
44. James Van Dyke

Mr. Van Dyke is the Founder and President of Javelin Strategy & Research ("Javelin"). Among other services, Javelin produces an annual study of identity theft in the United States. Under Mr. Van Dyke's leadership, Javelin's study provides a comprehensive analysis of identity fraud in the United States, which is used extensively by industry and other stakeholders. Mr. Van Dyke presents regularly to thought leaders on issues relating to identity theft and security.

Mr. Van Dyke will testify, from his perspective as an expert in identity theft, regarding the risk of injury to consumers whose personally identifiable information has been disclosed by LabMD without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure.

Dated: March 26, 2014

Respectfully submitted,



Alain Sheer

Laura Riposo VanDruff

Megan Cox

Margaret Lassack

Ryan Mehm

John Krebs

Jarad Brown

Complaint Counsel

Federal Trade Commission

600 Pennsylvania Avenue NW

Room NJ-8100

Washington, DC 20580

Telephone: (202) 326-2282 - (Cox)

Facsimile: (202) 326-3062

Electronic mail: mcox1@ftc.gov

CERTIFICATE OF SERVICE

I hereby certify that on March 26, 2014, I caused a copy of the foregoing document to be delivered *via* electronic mail and by hand to:

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

I certify that I caused a copy of the foregoing Complaint Counsel's Final Proposed Witness List to be served *via* electronic mail on:

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

Reed Rubinstein
Sunni Harris
William A. Sherman, II
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com
william.sherman@dinsmore.com
sunni.harris@dinsmore.com
Counsel for Respondent LabMD, Inc.

March 26, 2014


By: 
Megan Cox
Federal Trade Commission
Bureau of Consumer Protection

Exhibit D

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

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

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

RESPONDENT’S FINAL PROPOSED WITNESS LIST

Pursuant to the Court’s Revised Scheduling Order, dated October 22, 2013, Respondent hereby provides its Final Proposed Witness List to Complaint Counsel. This list identifies the fact witnesses who may testify for Respondent at the hearing in this action by deposition and/or investigational hearing transcript, declaration, or orally by live witness.

Subject to the limitations in the Scheduling Order and Revised Scheduling Order entered in this action, Respondent reserves the right:

A. To present testimony by deposition and/or investigational hearing transcript, affidavit, declaration, or orally by live witness, from the custodian of records of any party or non-party from whom documents or records have been obtained—specifically including, but not limited to, those parties and non-parties listed below—to the extent necessary to demonstrate the authenticity or admissibility of documents in the event a stipulation cannot be reached concerning the authentication or admissibility of such documents;

B. To present testimony by deposition and/or investigational hearing transcript, affidavit, declaration, or orally by live witness, from persons listed below and any other person that Complaint Counsel identifies as a potential witness in this action;

C. To amend this Final Proposed Witness List to be consistent with the Court's ruling on any pending motions, including any motions in limine filed in this matter;

D. To question the persons listed below about any topics that are the subjects of testimony by witnesses to be called by Complaint Counsel;

E. Not to present testimony by deposition and/or investigational hearing transcript, declaration, or live orally, from any of the witnesses listed below;

F. To question any person listed below about any other topics that the person testified about at his or her deposition or investigational hearing, or about any matter that is discussed in any documents to which the person had access and which are designated as exhibits by either party or which have been produced since the person's deposition was taken;

G. To present testimony by deposition and/or investigational hearing transcript, affidavit, declaration, or orally by live witness, from any persons, regardless whether they are listed below, to rebut the testimony of witnesses proffered by Complaint Counsel;

H. For any individual listed below as being associated with a corporation, government agency, or other non-party entity, to substitute a witness designated by the associated non-party entity; and

I. To supplement this Final Proposed Witness List as circumstances may warrant.

Subject to these reservations of rights, Complaint counsel's Final Proposed Witness list is

as follows:

1. Daniel Kaufman, Bureau of Consumer Protection's Rule 3.33 Witness

We expect that Mr. Kaufman will testify live about the FTC's regulatory scheme regarding data security, any published or unpublished FTC standards, guidelines or regulations which the FTC requires Covered Entities like LabMD to meet regarding the security of Protected Health Information from 2005 to the present; the initiation and evolution of the FTC's standards, guidelines and regulations regarding data security and what these regulations and guidelines required Covered Entities like LabMD to have in place at all relevant times from 2005 to the present; the media by which the FTC alerted or informed Covered Entities like LabMD that these standards, guidelines and regulations existed.

- 2. Robert Boback, Chief Executive Officer of Tiversa Holding Corporation (“Tiversa”)**
We expect that Mr. Boback will testify live, as Tiversa’s corporate designee, about Tiversa’s technology and its use on peer-to-peer file sharing protocols and networks; Tiversa’s communications with the FTC, Eric Johnson and Dartmouth; facts relating to the “P2P insurance aging file” referenced in Paragraph 17 of the Complaint; and other facts relating to the security incident alleged in Paragraphs 17-20 of the Complaint. We also expect that Mr. Boback will testify about facts relating to the documents produced in response to Complaint Counsel’s subpoena *duces tecum* to the organization that produced Tiversa’s document to the FTC in this action and the admissibility of those documents into evidence in the hearing in this action. We also expect that Mr. Boback will testify about any Civil Investigative Demands which resulted in the production of documents from Tiversa to FTC.
- 3. Eric Johnson, former Associate Dean of the Tuck School of Business at Dartmouth**
We expect that Mr. Johnson will testify live to the facts underlying his study entitled “Data Hemorrhages in the Health-Care Sector”; communications with the FTC, Tiversa, and/or Health and Human Services regarding LabMD, the 1718 file and his research methodology in general and specifically in relation to locating and downloading the 1718; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.
- 4. Allen Truett, former Chief Executive Officer of Automated PC Technologies, Inc.**
We expect that Mr. Truett will testify live about LabMD’s computer networks, including, but not limited to, remote access thereto; the products and/or services that he and his company, Automated PC Technologies, Inc., provided to LabMD, including but not limited to the security features of those products and/or services; the communications between LabMD and Mr. Truett or Automated PC Technologies, Inc.; the facts underlying and set forth in the affidavit that Mr. Truett executed on May 20, 2011, which LabMD submitted to Commission staff during the Part II investigation; and the facts relating to affirmative defenses asserted in the Answer.
- 5. Karina Jestes, Detective, Sacramento, CA Police Department**
We expect that Detective Jestes will testify by designation about facts relating to the security incident alleged in Paragraphs 10 and 21 of the Complaint; those consumers affected by the security incident alleged in Paragraphs 10 and 21 of the Complaint; facts relating to meetings and communications between her and the FTC; facts relating to the documents produced in response to Complaint Counsel’s subpoena *duces tecum* to the Custodian of Records of the Sacramento, CA Police Department in this action and the admissibility of those documents into evidence in the hearing in this action.
- 6. Robert Hyer, former LabMD IT Manager and former LabMD contractor**
We expect that Mr. Hyer will testify live about LabMD’s computer networks, including, but not limited to, hard ware and soft ware, remote access thereto; LabMD’s security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; and facts relating to affirmative defenses asserted in the Answer.

7. Jeff Martin, LabMD IT employee and former LabMD contractor

We expect that Mr. Martin will testify by designation about LabMD's computer networks, including, but not limited to, hard ware and soft ware, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.

8. Allison Simmons, former LabMD IT employee

We expect that Ms. Simmons will testify by designation about her knowledge of LabMD's searches for the 1718 file on P2P networks; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.

9. Chris Maire, former LabMD employee

We expect that Mr. Maire will testify by designation about LabMD's computer networks, including, but not limited to, hard ware and soft ware, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.

10. John Boyle, former LabMD employee

We expect that Mr. Boyle will testify live about LabMD's computer networks, including, but not limited to, remote access thereto; hard ware and soft ware, LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.

11. Michael Daugherty, President CEO of LabMD, Inc.

We expect that Mr. Daugherty will testify live about LabMD's computer networks; LabMD's security policies and practices, and employee training; LabMD employees; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.

12. Lou Carmichael, former LabMD consultant

We expect that Ms. Carmichael will testify by designation about LabMD's security policies and practices, hard ware and soft ware, compliance program, and employee training; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; and facts relating to affirmative defenses asserted in the Answer.

13. Rick Wallace, former Tiversa Employee

We expect that Mr. Wallace will testify live about Tiversa's technology and its use with peer-to-peer file sharing applications and networks; Tiversa's communications with the Federal Trade Commission ("FTC") and Dartmouth College; facts relating to the "P2P insurance aging file" as referenced in Paragraph 17 of the Complaint; Mr. Wallace's and Tiversa's participation and role in Dartmouth's research for the article by Eric Johnson, titled; "Data Hemorrhages in the Health-Care Sector."

14. Chris Gormley, Tiversa Employee

We expect that Mr. Gormley will testify by designation about Tiversa's technology and its use with peer-to-peer file sharing applications and networks; Tiversa's communications with the Federal Trade Commission ("FTC") and Dartmouth College; facts relating to the "P2P insurance aging file" as referenced in Paragraph 17 of the Complaint; Mr. Gormley's and Tiversa's participation and role in Dartmouth's research for the article by Eric Johnson, titled; "Data Hemorrhages in the Health-Care Sector."

15. Rosalind Woodson, Former LabMD Employee

We expect that Rosalind Woodson will testify live about her use of a P2P file sharing application on her work station computer and her knowledge of LabMD's policies regarding such use, as well as her knowledge of the "1718 File."

16. David Lapidés, Detective Sandy Springs, GA Police Department

We expect that Detective Lapidés will testify by designation about his communications with LabMD and the Bureau of Consumer Protection and documents provided to him relating to the security incident alleged in Paragraph 21 of the Complaint; or any other matters as to which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. Detective Lapidés will also testify about facts relating to documents that were produced in response to Complaint Counsel's subpoena *duces tecum* to the Sandy Springs, GA Police Department in this action, and the admissibility of those documents into evidence in the hearing in this action.

17. Curt Kaloustian, former LabMD IT employee

We expect that Mr. Kaloustian will testify live about his knowledge of LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; Respondent's affirmative defenses, or the proposed relief.

18. Kim Gardner, former LabMD Executive Assistant

We expect that Ms. Gardner will testify by designation about LabMD's security policies and practices, and employee training; the protected health information to which she had access; information relating to the wind down of LabMD's business operations and the corresponding relocation of LabMD's business premises; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint

Counsel about which she has knowledge; or any other matters as to which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

19. Peter Sandrev, Broadvox employee, Cypress Communications, LLC ("Cypress") designee

We expect that Mr. Sandrev will testify by designation about LabMD's computer networks, including, but not limited to the products and/or services that Cypress provided to LabMD, including but not limited to any security features of those products and/or services; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which Cypress has knowledge; or any other matters as to which Cypress has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. He will also testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to Cypress in this action, and the admissibility of those documents into evidence in the hearing in this action.

20. Eric Knox, former LabMD sales employee

We expect that Mr. Knox will testify by designation about LabMD's computer networks, including, but not limited to remote access thereto; LabMD's security policies and practices, and sales employee training; the protected health information to which he and other LabMD sales employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which he has knowledge; or any other matters about which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

21. Kevin Wilmer, Investigator, Federal Trade Commission, Bureau of Consumer Protection, Division of Privacy and Identity Protection

We expect that Mr. Wilmer will testify by designation about the process used to identify the individuals listed in Appendix A (designated as "CONFIDENTIAL") to Complaint Counsel's Initial Disclosures as "Individuals Associated with 9-Digit Numbers Listed in the Day Sheets Referenced in Paragraph 21 of the Complaint Whose Names Are Not Listed in Those Day Sheets," which has been produced at FTC-010907, as well any other issues addressed in his deposition.

22. Lawrence Hudson, former LabMD sales employee

We expect that Ms. Hudson will testify by designation about LabMD's computer networks, including, but not limited to remote access thereto; LabMD's security policies and practices, and sales employee training; the protected health information to which she and other LabMD sales employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel as to which she has knowledge; or any other matters as to which she has

knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

23. Letonya Randolph, Midtown Urology, PC ("Midtown Urology") employee, Midtown Urology designee

We expect that Ms. Randolph will testify by designation about Midtown Urology's relationship and communications with LabMD; computer hardware and software provided to Midtown Urology by LabMD, and the maintenance thereof; the transmission of protected health information between Midtown Urology and LabMD, if any; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which Midtown Urology has knowledge; or any other matters about which Midtown Urology has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. She will also testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to Midtown Urology in this action, and the admissibility of those documents into evidence in the hearing in this action.

24. Nicotra Harris, former LabMD finance or billing employee

We expect that Ms. Harris will testify by designation about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which she and other LabMD billing employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which she has knowledge; or any other matters about which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

25. Jeremy Dooley, former LabMD Communications Coordinator and IT employee

We expect that Mr. Dooley will testify by designation about LabMD's computer networks, including, but not limited to, hard ware and soft ware; remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; LabMD's IT related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which he has knowledge; or any other matters about which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

26. Jerry Maxey, Southeast Urology Network ("S.U.N.") employee, S.U.N. designee

We expect that Mr. Maxey will testify by designation about S.U.N.'s relationship and communications with LabMD; computer hardware and software provided to S.U.N. by LabMD, and the maintenance thereof; the transmission of protected health information between S.U.N. and LabMD; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which S.U.N. has knowledge; or any other matters about which S.U.N. has knowledge that are relevant to

the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief. He will also testify about facts relating to the documents produced in response to Complaint Counsel's subpoena duces tecum to S.U.N. in this action, and the admissibility of those documents into evidence in the hearing in this action.

27. Jennifer Parr, former LabMD IT employee

We expect that Ms. Parr will testify by designation about LabMD's computer networks, including, but not limited to, hardware and software; remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which she and other LabMD employees had access; LabMD's IT related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which she has knowledge; or any other matters about which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

28. Karalyn Garrett, former LabMD finance or billing employee

We expect that Ms. Garrett will testify by designation about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which she has knowledge; or any other matters about which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

29. Patricia Gilbreth, former LabMD finance or billing employee

We expect that Ms. Gilbreth will testify by designation about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which she has knowledge; or any other matters about which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

30. Patrick Howard, former LabMD IT employee

We expect that Mr. Howard will testify by designation about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which he has knowledge; or any other matters about which he

has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

31. Sandra Brown, former LabMD finance or billing employee

We expect that Ms. Brown will testify by designation about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which she and other LabMD employees had access; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in her deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which she has knowledge; or any other matters about which she has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

32. Brandon Bradley, former LabMD IT employee

We expect that Mr. Bradley will testify by designation about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the protected health information to which he and other LabMD employees had access; LabMD's IT-related expenditures; facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint; any other issues addressed in his deposition; any documents introduced into evidence by Respondent or Complaint Counsel about which he has knowledge; or any other matters about which he has knowledge that are relevant to the allegations of the Complaint, Respondent's affirmative defenses, or the proposed relief.

33. Erick Garcia

We expect that Mr. Garcia will testify by designation about facts relating to the security incident alleged in Paragraph 21 of the Complaint.

34. Adam Fisk

We expect Adam Fisk to testify live and give an expert opinion about the technology behind the program known as LimeWire; the operation of peer to peer networks; the adequacy of LabMD's network security hardware, software policies practices and procedures; and to offer rebuttal testimony with regard to Complaint Counsel's expert Rachel Hill's opinion.

s/ William A. Sherman, II

Reed D. Rubinstein, Esq.

William A. Sherman, II, Esq.

Dinsmore & Shohl, LLP

801 Pennsylvania Ave., NW Suite 610

Washington, DC 20004

Phone: (202) 372-9100

Fax: (202) 372-9141

Email: reed.rubinstein@dinsmore.com

william.sherman@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: (202) 499-4232
Fax: (202) 330-5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and
and administrative proceedings before federal
agencies.
Counsel for LabMD, Inc.

CERTIFICATE OF SERVICE

I certify that on April, 9 2014 I caused a copy of the foregoing Respondent's Final Proposed Witness List to be served via courier on:

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

Dated: April 9, 2014

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

554316v1