

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



_____))
In the Matter of)) PUBLIC
))
LabMD, Inc., a corporation))
Respondent.))
_____))
))

RESPONDENT LABMD, INC.’S MOTION TO ADMIT SELECT EXHIBITS

Pursuant to Additional Provision 16 to this Court’s Scheduling Order, and Commission Rules 3.22 and 3.43 (16 C.F.R. §§ 3.22, 3.43), and the Court’s June 1, 2015 Order, Respondent LabMD, Inc. (“LabMD”) hereby moves to admit select exhibits. As detailed below, the proffered evidence is reliable, material, and relevant to the veracity of the testimony provided by Tiversa, Inc. (“Tiversa”), the allegations made by the Federal Trade Commission (“FTC”) with respect to the “spread” of the 1718 File on P2P networks, LabMD’s defense, and other core issues in this case.

The select exhibits moved for admission into evidence are listed in Appendix A, which is attached hereto and made a part hereof.¹

I. Standard of Review.

Relevant, material, and reliable evidence shall be admitted. *See* Commission Rule 3.43. Hearsay that is “relevant, material, and bears satisfactory indicia of reliability so that its use is fair” also should be admitted. Commission Rule 3.43(b); *see also In re Polyvore Int’l, Inc.*, No. 9327, 2010 FTC LEXIS 62, at *6-7 (July 10, 2010) (noting that hearsay evidence may be received in FTC proceedings). However, a document that is not admitted for the truth of the matter asserted, by definition, is not hearsay. Fed. R. Evid. 801.

¹ A disc with the selected exhibits is attached with Appendix A for the Court’s convenience.

“The Federal Rules of Evidence define relevancy to include evidence that has *any* tendency to make a fact of consequence to the determination of the action more or less probable ... [and] ‘the federal courts are unanimous in holding that the definition of relevant is expansive and inclusive, and that the standard for admissibility is very low.’” *In the Matter of OSF Healthcare System*, No. 9349, 2012 FTC LEXIS 75, at *3 (Apr. 4, 2012) (citation & notes omitted).²

Under the Administrative Procedure Act (“APA”), an administrative law judge may not issue an order “except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the reliable, probative, and substantial evidence.” *In the Matter of ECM Biofilms*, No. 9358, 2015 FTC LEXIS 22, at *9 (FTC Jan. 28, 2015) (citing Administrative Procedures Act, 5 U.S.C. § 556(d)). Indeed, Rule 3.43(d) directs the administrative law Judge to control the presentation of evidence so as to make the presentation “effective for the ascertainment of the truth.” 16 C.F.R. § 3.43(d).

II. General Nature of the Exhibits to be Admitted.

The documents at issue are reliable and clearly relevant to the facts of the case. The majority of the documents have been produced by FTC in response to FOIA requests. The records also emanate from the production of documents by and testimony of Richard Wallace, the Tiversa whistleblower who testified on May 5, 2015 before this Court. There is no reason to doubt the authenticity of any of the exhibits to be moved into evidence.

The majority of the exhibits (described under **Categories 1-5** *infra*) are documents produced to undersigned counsel by FTC in response to proper Freedom of Information Act (“FOIA”) requests. *See* Certification of Records of Regularly Conducted Activity of Cause of

² The Federal Rules of Evidence are persuasive authority for FTC adjudicative proceedings. *Id.* at n.2 (citation omitted).

Action Institute, attached hereto as Exhibit 1.³ Specifically, FTC responded to the FOIA requests in the regular course of agency operations, which FTC was statutorily required to do under the APA. These documents are offered to show, as a general matter, the state of mind and actions of FTC as an agency responding to a Congressional inquiry involving a material government witness who supplied FTC with evidence and testimony in furtherance of its pending adjudication against LabMD. For these reasons (and as discussed in greater detail below), the documents should be admitted.⁴

Moreover, in anticipation that Complaint Counsel will assert that this motion is untimely because, among other reasons, the documents at issue were not on a prior exhibit list, LabMD notes that: 1) these documents, which are responsive to LabMD's First Request for Production of Documents Nos. 1, 4-7, 11-12 (*see* Ex. 2, LabMD's First Set of Requests for Production of Documents to FTC, at 11 (Dec. 24, 2013)), were never produced by Complaint Counsel in this case, despite its ongoing duty to supplement; and 2) LabMD did not receive some of the documents until May 2015, when FTC produced them in response to FOIA request(s). In addition, LabMD offers this evidence for the Court's consideration in properly effectuating the "ascertainment of the truth." *See* Rule 3.43(d).

³ *See also* Joint Stipulations of Fact, Law, and Authenticity, at 4 (May 14, 2014) (parties stipulating to the authenticity of all exhibits, with limited specified exceptions).

⁴ *See Morgan v. U.S. Dep't of Justice*, 923 F.2d 195, 198 (D.C. Cir. 1991) ("[T]he potential availability of criminal and civil discovery in no way bars an individual from obtaining information through FOIA where no exemption otherwise applies."). "Indeed, there are situations in which FOIA will permit access to information that would not be available through discovery." *Id.* (citing *North v. Walsh*, 881 F.2d 1088, 1096 (D.C. Cir. 1989); *see also Roth v. U.S. Dep't of Justice*, 642 F.3d 1161, 1183 (D.C. Cir. 2011) (citing *Morgan* and *North*)).

III. Specific Discussion of the Exhibits to be Admitted.

Category 1

Miscellaneous exhibits

RX552-RX553: May 7, 2014 hearing in Atlanta, Georgia and the expert report Cliff Baker: relevant, material, reliable evidence of the data security standards applicable to LabMD during 2005-2010 as a HIPAA-covered entity. This is relevant because Baker opines that Rachel Hill's proposed data security standards are inconsistent with applicable standards under HIPAA. Hearing Tr. (N.D. Ga.), at 64:25 – 65:13 (May 7, 2014); Baker Report, at 1-13 (rec'd in evidence). RX553: LabMD certificate is relevant for the same reasons. *See* App. A. LabMD has contended throughout this case as a material fact that it is a HIPAA-covered entity which did not commit any HIPAA-related data security violations.

RX554: Self-authenticating, relevant, and probative FTC CID to the Privacy Institute, which included the insurance aging file at the center of FTC's case. *See* Wallace, Tr. at 1352:17-25 – 1353:1-6, 16-20; RX644 at 4, 54-8 (OGR Report).

RX615-616: Self-authenticating, relevant, and probative responses to Questions for the Record by FTC regarding data security to U.S. House Subcommittee on Commerce, Manufacturing & Trade on Feb. 4, 2014 (July 11 & 16-17, 2014). FTC's lack of standards for data security in the medical industry, and specifically regarding P2P networks, is a material fact(s) in this case. *See* Complaint, at ¶¶13-20; FTC Staff Report at 20 (June 2005); Prepared Statement of Mary Engle, at 1-12 (July 24, 2007).

RX644: Relevant, self-authenticating, material, probative January 2, 2015 Staff Report prepared for OGR Chairman Darrell E. Issa regarding Tiversa and FTC in the LabMD matter, entitled, "*Tiversa, Inc.: White Knight or High-Tech Protection Racket?*" This exhibit is not

offered for the truth of the matters set forth therein. This document is the culmination of numerous exhibits involving the 1718 File and the nature of FTC's use of Tiversa's evidence in the case against LabMD. It is self-authenticating and probative of these issues, as well as LabMD's defenses in this case. *See* Complaint at ¶¶ 10-20, 22-23; Answer at ¶¶ 10-20, 22-23; Answer, LabMD's Affir. Def. at 6-7; CX0019; Wallace, Tr. at 1341:12-25, 1342:1-6, 1432:10-25 – 1433:1-12, 1352:17-25 – 1353:1-6, 16-20, 1358:16-25 – 1359:1-14, 1363:11-14, 1367:7-18, 1368: 3-17, 23-25 — 1369:1-25, 1370:1-2, 1374:14 — 1378:2, 1378:18 — 1379:11, 1379:22 — 1385:3, 1385:3-24; LabMD's Motion to Disqualify Commissioner Edith Ramirez; LabMD's Motion For Leave to Supplement the Record in Support of Its Motion to Disqualify Commissioner Ramirez; Hill (CX0740), at 1, 15; Van Dyke (CX0741), at 2, 4, 7, 8; Kam (CX0742), at 6, 9, 18, 19; Shields (CX0738), at 3, 25.

RX649: Relevant news article regarding HHS's decision not to investigate or prosecute LabMD (Sept. 9, 2013). The jurisdiction of FTC under Section 5 over a HIPAA-covered entity is a material fact in this case. *See* Ex. 3, Declaration of Michael Pepson, *LabMD, Inc. v. FTC* (Case 1:14-cv-00810-WSD) (N.D. Ga.) (Mar. 20, 2014).

RX653: Relevant emails between Samuel Hopkins/Tiversa and Johnson regarding data for Johnson's study. The foundation for this exhibit is Johnson's deposition testimony. *See* CX0720, at 78-83 (Feb. 18, 2014).

RX654: Relevant testimony of Boback before the U.S. House Subcommittee on Commerce, Trade, and Consumer Protection, which is a public document. The foundation for this exhibit is the deposition testimony of Boback on November 21, 2013, and Wallace's trial testimony. *See* CX703, at 143-59 (Nov. 21, 2013); Wallace, Tr. at 1341:12-25, 1342:1-6, 1432:10-25 – 1433:1-12 (VOL. IX) (May 5, 2015) (PUBLIC).

RX656: Boback deposition exhibits relevant to CX0019 and FTC's representations to Congress. *See* Boback, Dep. Tr. at 43-47 (June 7, 2014). This exhibit is relevant, reliable, public, and probative evidence of what Boback stated to Computer World on or about February 26, 2010. The article is not offered for the truth of what Boback stated.

Category 2

Internal FTC emails and communications regarding OGR's letters dated June 11, 2014 and June 17, 2014

RX587: Relevant public document of FTC's response to OGR's June 11 letter stating that Congress was investigating Tiversa and FTC. These exhibits are admissions of FTC employees regarding material facts at issue in this case. *See* Wallace, Tr. at 1385:13-24, 1352:17-25 – 1353:1-6, 16-20; RX644 *infra*, at 54-62, 56 n.173.

RX592-94; RX596; RX613-14; RX617; RX619; RX621-22; RX625: Relevant and reliable email communications regarding FTC responses to OGR's June 11, 2014 letter to Commissioner Ramirez, and to OGR's June 17, 2014 letter to FTC Acting Inspector General Kelly Tshibaka. These exhibits also include communications between Congressional staffers and FTC employees regarding a pending adjudicative matter, and the lack of FTC standards regarding data practices and "unfairness" under Section 5. These exhibits are admissions of FTC employees regarding material facts at issue in this case.⁵

⁵ These communications are relevant also because the records are evidence of FTC's public positions, and contrary internal actions and discussions, regarding the viability of Tiversa's evidence in the LabMD matter, as well as FTC's view of Tiversa's credibility as the sole source of evidence regarding a "likely" cause of *substantial injury* under Section 5 of the FTC Act, which FTC has the burden of proving in this case. FTC/Complaint Counsel have never disavowed or otherwise qualified the testimony of Tiversa or Robert Boback in this case that the insurance aging file proliferated on P2P networks as reflected in CX0019. *See* Complaint, at ¶¶10-20, 22-23; Answer, at ¶¶10-20, 22-23; Answer, LabMD's Affir. Def. at 6-7; CX0019; **RX644**, at 7-72; Wallace, Tr. at 1358:16-25 – 1359:1-14, 1363:11-14, 1368:23-25 — 1369:1-25, 1370:1-2, 1374:14 — 1378:2, 1378:18 — 1379:11, 1379:22 — 1385:3, LabMD's Motion to Disqualify Commissioner Edith Ramirez; LabMD's Motion to Supplement the Record in Support of Its Motion to Disqualify Commissioner Ramirez.

Additionally, **RX622** is relevant to FTC's lack of standards regarding data security and "unfairness" under Section 5 of the FTC Act. **RX625** is an email exchange between an FTC employee and an OGR Deputy Staff Director regarding an improper request by the FTC employee for a transcript of Boback's June 5, 2014 testimony before OGR. See **RX644** *infra*, at 4-72.

Category 3

Internal FTC emails and communications regarding OGR's July 18, 2014 letter

RX584; RX586; RX588; RX611-12; RX618; RX620; RX623-24; RX626-28: Relevant and reliable email communications regarding FTC's response to OGR's July 18, 2014 letter to Commissioner Ramirez. These exhibits also include communications between Congressional staffers and FTC employees regarding a pending adjudicative matter, and the lack of FTC standards regarding data practices and "unfairness" under Section 5.⁶

Category 4

Internal FTC emails and communications regarding OGR's December 1, 2014 letter

RX630-32; RX634-35; RX637-40; RX643: Relevant and reliable email communications regarding FTC's response to OGR's December 1, 2014 letter to Commissioner Ramirez. These exhibits include communications between FTC employees regarding a pending adjudicative matter, and the lack of FTC standards regarding data practices and "unfairness" under Section 5.⁷

⁶ See *supra* note 5.

⁷ See *supra* note 5.

Category 5

FTC communications

RX583: Relevant and reliable October 2014 email communications between DAEO White, Senior FTC Leadership, and LabMD Complaint Counsel, and voicemail verifications from August 2014.

RX590-91: Relevant and reliable email communications regarding FTC's responses to OGR's June 11 and June 17, 2014 letters to Commissioner Ramirez and FTC's IG. This exhibit includes FTC employees discussing a pending adjudicative matter, and an upcoming meeting on Capitol Hill with Rep. Terry regarding Tiversa.

RX583 and RX590-91: Relevant evidence of FTC's public positions, and contrary internal actions and discussions, regarding the viability of Tiversa's evidence in the LabMD matter, as well as FTC's view of Tiversa's credibility as the sole source of evidence regarding the insurance aging file.⁸

RX595; RX597-99; RX600; RX602-04; RX606: Relevant and reliable email communications showing FTC Complaint Counsel in the LabMD matter, as well as FTC Senior Leadership and officials, contacting DAEO White with regard to the LabMD matter. These exhibits also contain email communications by and between FTC Senior Leadership and FTC employees, including but not limited to Complaint Counsel, regarding the LabMD case. These exhibits are admissions of FTC regarding material facts in this case.

RX610: Relevant and reliable email communications showing FTC Complaint Counsel in the LabMD matter, as well as FTC Senior Leadership and officials, discussing the disqualification of Commissioner Julie Brill on December 24, 2013.

⁸ See *supra* note 5.

RX659: Relevant public document of FTC's claims regarding the dangers of P2P networks for the period 2005-2010. *See* Complaint, at ¶¶13-20; FTC Staff Report, at 20 (June 2005); Prepared Statement of Mary Engle, at 1-12 (July 24, 2007) (OGR).

IV. Conclusion.

For the reasons set forth above, LabMD's Motion should be granted.

Dated: June 12, 2015

Respectfully submitted,

/s/ Prashant K. Khetan

Daniel Z. Epstein, Esq.

Prashant K. Khetan, Esq.

Patrick J. Massari, Esq.

Erica L. Marshall, Esq.

Cause of Action

1919 Pennsylvania Ave., NW Suite 650

Washington, DC 20006

Phone: (202) 499-4232

Facsimile: (202) 330-5842

Email: prashant.khetan@causeofaction.org

/s/ Reed D. Rubinstein

Reed D. Rubinstein, Esq.

William A. Sherman, II, Esq.

Dinsmore & Shohl, LLP

801 Pennsylvania Ave., NW Suite 610

Washington, DC 20004

Phone: (202) 372-9100

Facsimile: (202) 372-9141

Email: reed.rubinstein@dinsmore.com

Counsel for Respondent, LabMD, Inc.

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

In the Matter of)
)
LabMD, Inc.,)
a corporation.)
)
_____)

DOCKET NO. 9357

**[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.’S
MOTION TO ADMIT SELECT EXHIBITS**

Upon consideration of Respondent’s Motion to Admit Select Exhibits, and designated under Appendix A to said Motion, and in consideration of the entire Record in this case,

IT IS HEREBY ORDERED that Respondent’s Motion to Admit Select Exhibits be and the same is hereby GRANTED; and it is further

ORDERED that the Exhibits identified in Appendix A shall be admitted into evidence:

SO ORDERED:

D. Michael Chappell
Chief Administrative Law Judge

Date: _____

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

In the Matter of)
)
LabMD, Inc.,)
a corporation.)
)
_____)

DOCKET NO. 9357

STATEMENT REGARDING MEET AND CONFER

LabMD, Inc. respectfully submits this Statement, pursuant to Additional Provision 4 of the Scheduling Order. Prior to filing the attached Motion To Admit Select Exhibits, on June 5, 2015, counsel for LabMD (Patrick J. Massari and Erica L. Marshall) conferred with Complaint Counsel (Laura Riposo VanDruff and Jarad Brown) regarding the subject of these motions. Complaint Counsel advised that it opposes LabMD’s Motion, save RX651 and RX658 (which Complaint Counsel has already moved into evidence as CX0447 and CX0034, respectively).

Dated: June 12, 2015

Respectfully submitted,

/s/ Patrick J. Massari
Daniel Z. Epstein, Esq.
Prashant K. Khetan, Esq.
Patrick J. Massari, Esq.
Erica L. Marshall, Esq.
Cause of Action
1919 Pennsylvania Ave., NW Suite 650
Washington, DC 20006
Phone: (202) 499-4232
Facsimile: (202) 330-5842
Email: prashant.khetan@causeofaction.org

/s/ Reed D. Rubinstein

Reed D. Rubinstein, Esq.

William A. Sherman, II, Esq.

Dinsmore & Shohl, LLP

801 Pennsylvania Ave., NW Suite 610

Washington, DC 20004

Phone: (202) 372-9100

Facsimile: (202) 372-9141

Email: reed.rubinstein@dinsmore.com

Counsel for Respondent, LabMD, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on June 12, 2014, I delivered via electronic mail and caused to be hand-delivered a copy of the foregoing document with the Office of the Secretary:

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

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

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

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

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Jarad Brown, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Room CC-8232
Washington, D.C. 20580

Dated: June 12, 2015

By: /s/Patrick J. Massari

CERTIFICATE OF ELECTRONIC FILING

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

Dated: June 12, 2015

By: /s/Patrick J. Massari

APPENDIX A

Exhibit No.	Description	Bates Nos.
-------------	-------------	------------

Category 1

Miscellaneous Exhibits

RX552	Expert report of Cliff Baker (Apr. 11, 2014) and Hearing Transcript (May 7, 2014), <i>LabMD, Inc. v. FTC</i> (Case 1:14-cv-00810-WSD) (“N.D. Ga. Case”)	0001 – 112
RX553	HHS/CMS Certificate of Compliance: LabMD, Inc. 2003-2013 (Ex. 1 to Daugherty Decl.) (Mar. 20, 2014), N.D. Ga. Case	0113 – 114
RX554	C.I.D. to Privacy Institute (July 10, 2009-Aug. 13, 2009)	0115 –127
RX615	FTC responses to Questions for the Record to U.S. House Subcomm. on Commerce, Manuf. & Trade on Feb. 4, 2014) (July 11, 2014)	0614 – 623 (4/30/15)
RX616	FTC responses to Questions for the Record to U.S. House Subcomm. on Commerce, Manuf. & Trade on Feb. 4, 2014) (July 16-17, 2014)	0624 – 633 (4/30/15)
RX644	OGR Staff Report dated January 2, 2015 prepared for OGR Chairman Darrell E. Issa: “ <i>Tiversa, Inc.: White Knight or High-Tech Protection Racket?</i> ”	0756 – 854
RX649	News article re HIPAA (Sept. 9, 2013)	Exhibit 1 to Pepson Decl. ND Ga. Case
RX653	Emails between Hopkins and Johnson (Mar. 2008)	Johnson Dep. Ex. RX10 (Feb. 18, 2014)
RX654	Boback testimony/House Subcomm. Commerce, Trade, & Consumer Protection (May 4, 2009)	Boback Dep. Ex. RX1 (Nov. 21, 2013)
RX656	Computer World article	Robert Boback Dep. RX536 (June 7, 2014)

Ex. No.	Description	Bates Nos.
---------	-------------	------------

Category 2

Internal FTC emails and communications regarding OGR's letter of June 11, 2014 to Commissioner Ramirez, and June 17, 2014 to Acting Inspector Gen. Kelly Tshibaka requesting an investigation into FTC and Tiversa in the LabMD matter

RX587	Letter dated June 13, 2014 from FTC Sec'y Clark to OGR/Issa	0436 – 439
RX592	FTC email chain between Acting FTC IG Tshibaka to Hipsley, DAEO White, & OCR Dir. Bumpus	0471 – 472
RX593	Email chain: Sec'y Clark, DAEO White, COS Hipsley, Atty. Advisor Burstein	0473 – 487
RX594	Email chain reflecting Comm'r Ramirez's edits/input into June 13, 2014 response letter	0488 – 489
RX596	Email chain by: Comm'r Ramirez, DAEO White, Sec'y Clark, OCR Staff	0491 – 501
RX613	Email chain: Shannon Taylor (U.S. House) & OCR staffer Kim Vandecar	0607 – 611
RX614	Email chain: Taylor & Vandecar (June 18, 2014)	0612 – 613
RX617	Email: Taylor to Vandecar (June 18, 2014)	0634
RX619	Email from Vandecar to OGR staff (June 13, 2014)	0638 – 639
RX621	Email chain: FTC Staff and OGR Staff (June 11-13, 2014)	0642 – 643
RX622	Emails: Joseph Wender (Sen. Markey staffer) and Vandecar re FTC data security standard (June 13, 2014)	0644
RX625	Email from Vandecar to Mark Marin (OGR Deputy Staff Dir.) (June 16-17, 2014)	0648 – 649

Ex. No.	Description	Bates Nos.
---------	-------------	------------

Category 3

Internal FTC emails and communications regarding OGR's July 18, 2014 letter to Commissioner Ramirez, and OGR's July 24, 2014 hearing entitled "The Federal Trade Commission and its Section 5 Authority: Prosecutor, Judge, and Jury"

RX584	Emails regarding OGR's July 18, 2014 letter to Comm'r Ramirez	0420 – 433
RX586	Emails regarding OGR's June 11 & July 18, 2014 letters to Comm'r Ramirez	0435
RX588	Emails regarding OGR's July 18, 2014 letter to Comm'r Ramirez (July 18-20, 2014)	0440 – 458
RX611	Emails: Ellen Doneski (Sen. Jay Rockefeller/Senior Staff) to Comm'r Ramirez regarding Sen. Rockefeller's July 23, 2014 letter	0596 – 599
RX612	Email chain: Hill staffers and OCR Dir. Bumpus/OCR Staff	0603 – 606
RX618	FTC response letter by Sec'y Clark to OGR's July 18, 2014 letter	0635 – 637
RX620	Email: OCR Staff, Daniel Kaufman, and OGR Staff	0640 – 641
RX623	Emails: FTC Staff and OGR Staff re FTC's response to OGR's July 18, 2014 letter (July 21, 2014)	0645 – 646
RX624	Emails: OCR Staff and OGR Staff (July 23, 2014)	0647
RX626	Email: OGR staffer Patrick Satalin (Rep. Peter Welch) to Aaron Burstein (Atty. Advisor to Comm'r Brill) regarding July 24, 2014 OGR hearing	0650
RX627	Email: Jennifer Barblan (OGR Senior Counsel) to OCR staffer Claudia Simons transmitting OGR's July 18, 2014 letter (July 18, 2014 12:28 PM)	0651 – 658
RX628	Email: Matthew Smith (FTC DPIP) to OGR transmitting file 2014072.zip/708,171.51 KB of FTC data/records	0659 – 660 (4/30/15)

Ex. No.	Description	Bates Nos.
---------	-------------	------------

Category 4

Internal FTC emails and communications regarding OGR's December 1, 2014 letter to Commissioner Ramirez

RX630	Dec. 1, 2014 letter from OGR to Comm'r Ramirez with select attachments	0685 – 702
RX631	Email: Laura Riposo Van Druff to Chief ALJ D. Michael Chappell transmitting the FTC's December 16, 2014 response letter (Dec. 18, 2014)	0719 – 720 (5/14/2015)
RX632	Email: Van Druff to David C. Shonka re LabMD matter (Dec. 2, 2014)	0721 (5/14/2015)
RX634	Emails: Bumpus and Van Druff regarding FTC's December 16, 2014 response letter (Dec. 16, 2014)	0723 – 725 (5/14/2015)
RX635	Email: OGR to FTC/OCR transmitting OGR's December 1, 2014 letter (Dec. 1, 2014)	0726 – 727 (5/14/2015)
RX637	Email: Bumpus to Shonka & Vandecar (Dec. 3, 2014)	0730 (5/14/2015)
RX638	Emails: FTC officials regarding OGR's December 1, 2014 letter (Dec. 1-2, 2014)	0731 – 732 (5/14/2015)
RX639	Email: Sec'y Clark to Staff regarding OGR's December 1, 2014 letter (Dec. 19, 2014)	0733 – 734 (5/14/2015)
RX640	Emails: Comm'r Ramirez and COS Heather Hipsley (Dec. 10, 2014; Dec. 15, 2014)	0735 (5/14/2015)
RX643	Emails: Sec'y Clark and Bumpus (Dec. 15, 2015)	0739 (5/14/2015)

Ex. No.	Description	Bates Nos.
---------	-------------	------------

Category 5
FTC communications

RX583	Emails: DAEO White from Complaint Counsel, FTC leadership (Oct. 2014); voicemail verifications (Aug. 2014)	0346 –350 (4/30/15)
RX590	Emails: Mithal/DAEO White/Staff Atty. Blodgett (June 23-27, 2014)	0460 – 461 (4/30/15)
RX591	Emails: Comm’r Ramirez, DAEO White, Gen. Counsel Jon Nuchterlein (June 20, 2014); internal FTC email from Mithal to DAEO White re June 19, 2014 internal meeting	0469 – 470 (4/30/15)
RX595	Email: Alain Sheer and DAEO White (Nov. 5, 2014)	0490 (4/30/15)
RX597	Emails: Van Druff, Sheer and DAEO White (June 19, 2014)	0502 – 503 (4/30/15)
RX598	Email: Van Druff to DAEO White (Nov. 5, 2014)	0504 (4/30/15)
RX599	Notice of voicemail: DPIP Ass’t Dir. Schoshinski to DAEO White (June 9, 2014)	0505 (4/30/15)
RX600	Emails: Comm’r Ramirez/COS Hipsley to DAEO White, OCR Dir. Bumpus, Dir. Pub. Affairs & Comms. Justin Cole (May 30, 2014); Sheer and DAEO White (May 31 & June 2, 2014)	0506 (4/30/15)
RX602	Email: Van Druff to DAEO White (Mar. 25, 2014)	0508 (4/30/15)
RX603	Email: FTC witness Ruth Yodaiken and DAEO White (Mar. 14, 2014)	0509 (4/30/15)
RX604	Email: Van Druff to DAEO White (Nov. 4, 2014)	0510 (4/30/15)
RX606	Emails: FTC Senior Leadership, DAEO White, and LabMD Complaint Counsel (Feb.-Mar. 2014)	0512 – 519 (4/30/15)
RX610	Emails: FTC Senior Leadership regarding Comm’r Brill’s disqualification (Dec. 17-18 & 26, 2013)	0542,0545, & 0570 (4/30/15)
RX655	Letter from Settlemyer to Boback (June 25, 2008)	Boback Dep. Ex. RX2 (Nov. 21, 2013)
RX659	Letter from Mary K. Engle to George Searle, CEO LimeWire (Aug. 19, 2010)	FTC File No. 082- 3046, 8.19.2010 (FTC- 013897- 013898)

**SELECT EXHIBITS
TO BE ADMITTED**

CATEGORY 1

Miscellaneous Exhibits

RX552

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

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

EXPERT OPINION DECLARATION OF CLIFF BAKER

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

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

- a. Director in the Healthcare Information Security practice at PricewaterhouseCoopers. I led the security practice nationally for the Healthcare Consulting practice. I worked at PricewaterhouseCoopers for 14 years and consulted with clients nationally on implementing security programs and practices. An example of a project I led was a establishing a program that included four state healthcare associations. The program included meeting, discussing and educating over 50 organizations on adopting security measures to comply with HIPAA.
- b. Chief Strategy Officer for HITRUST. I joined HITRUST in 2008 to lead the creation of the Common Security Framework, which is a healthcare industry framework based on globally recognized standards, such as ISO 27001/2 and NIST. A key objective of the framework is to provide a prescriptive and scalable reference for covered entities to determine reasonable and appropriate controls to implement for their organizations. The controls are tailored to the size and operations of the organization. I facilitated working sessions with over 200 security professionals from the healthcare

industry, security technology companies, consulting companies, and government entities in the development of the framework.

c. Founder and Managing Partner of Meditology Services.

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

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

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

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

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

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

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

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

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

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

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

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

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

Remember the Basics

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

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

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

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

- a. Confusing by introducing additional security principles (i.e., 7 security principles referenced by Dr. Hill) that are difficult to reconcile with the Administrative, Technical and Physical main structure of the HIPAA security rule.
- b. Not scalable in accordance with the Security Rule, and not taking account as required by the 1996 HIPAA Statute of "the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary). For example, the recommendation for file integrity monitoring requires expertise to implement and configure these solutions and can be even more resource intensive to understand, investigate and resolve alerts produced by the solution. In my experience, I very rarely observe adoption of this technology by small providers in the industry.
- c. More prescriptive than HIPAA or inconsistent with HHS guidance, including encryption at rest (an addressable requirement of 164.312(a)(1)), encryption in transit (an addressable requirement

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

- d. Contradictory to the guidance provided by HHS. For example, Dr. Hill almost exclusively focuses on technologies or technical processes for the risk assessment process (i.e., antivirus

applications, firewalls, various types of vulnerability scans, intrusion detection systems, penetration tests, file integrity monitoring, and other measures). This is inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process as outlined in the standard referenced by Dr. Hill: Special Publication NIST 800-30 Guide for Conducting Risk Assessments.

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

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

RX552

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

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

Executed on this 11 day of April, 2014.



CLIFF BAKER

CERTIFICATE OF SERVICE

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

Mail as follows:

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

This 11th day of April, 2014.

/s/ Burleigh L. Singleton _____
Counsel for Plaintiff

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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

LabMD, INC.)	
)	
Plaintiff,)	CIVIL ACTION FILE
)	NO. 1:14-CV-810-WSD
v.)	
)	ATLANTA, GEORGIA
FEDERAL TRADE COMMISSION)	
)	
Defendant.)	
_____)	

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE WILLIAM S. DUFFEY, JR.,
UNITED STATES DISTRICT JUDGE

Wednesday, May 7, 2014

APPEARANCES OF COUNSEL:

For the Plaintiff:	KILPATRICK TOWNSEND & STOCKTON LLP
	(By: Ronald L. Raider
	William D. Meyer)
	Burleigh Lavisky Singleton)
	DINSMORE & SHOHL LLP
	(By: Reed D. Rubinstein)
For the Defendant:	U.S. DEPARTMENT OF JUSTICE
	(By: Lauren Fascett
	Perham Gorji
	Joel Marcus)

*Proceedings recorded by mechanical stenography
and computer-aided transcript produced by*
NICHOLAS A. MARRONE, RMR, CRR
1714 U. S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
(404) 215-1486

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

I N D E X

<i>Witness</i>	<i>Page</i>
MICHAEL JOHN DAUGHERTY	
Direct (By Mr. Raider)	5
Cross (By Mr. Gorji)	32
Redirect (By Mr. Raider)	57
CLIFF BAKER	
Direct (By Mr. Meyer)	58

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Wednesday Morning Session

May 7, 2014

9:44 a.m.

-- -- --

P R O C E E D I N G S

-- -- --

(In open court:)

THE COURT: Good morning, everybody.

This is the hearing that is scheduled pursuant to my amended scheduling order which is dated April 9th this year. It's a hearing on the motion for preliminary injunction that's been requested by LabMD.

And absent anything that you want to discuss before we start, I would say let just get started. Any objection to doing that?

MR. RAIDER: No, Your Honor.

MS. FASCETT: No, Your Honor.

THE COURT: All right. And, LabMD, this is your hearing. You may begin.

MR. RAIDER: Thank you, Your Honor.

We would like to start by presenting some live testimony from Mr. Daugherty.

THE COURT: That would be fine.

MR. RAIDER: We also have Mr. Baker here.

Is it okay that he sits in the back or do you want

1 him out in the witness room?

2 THE COURT: Do you want him sequestered?

3 MS. FASCETT: I don't think that's necessary,
4 Your Honor.

5 THE COURT: I agree.

6 Okay. Let's begin, then.

7 (The oath is given by the Courtroom Deputy Clerk.)

8 MR. RAIDER: Your Honor, just as Mr. Daugherty is
9 getting some water, we have presented a notebook with all of
10 the exhibits that plaintiff has on its exhibit list, and we
11 will be using some of those in his examination.

12 So the witness has a copy, government counsel has a
13 copy, and I think a copy has been made available to you.

14 THE COURT: I have got it.

15 And let's make sure all the appearances are noted
16 on the record.

17 I guess we have Mr. Rubinstein, Mr. Singleton,
18 Mr. Meyer, Mr. Raider for LabMD; is that correct?

19 MR. RAIDER: Yes.

20 THE COURT: And for the FTC, Ms. Fascett, Mr. Gorji
21 is it?

22 MR. GORJI: Correct, Your Honor.

23 THE COURT: And Mr. Marcus, who I don't think has
24 made an appearance in the case.

25 MR. MARCUS: That's correct. For the FTC, I am

1 just serving as of counsel here. I would be happy to enter
2 an appearance if you would like.

3 THE COURT: Well, I mean, if you are just sitting
4 there because you are an observer and not in the case, that's
5 fine. But if you are in the case, you need to make an
6 appearance.

7 MR. MARCUS: I will do that, Your Honor.

8 THE COURT: And please do that today.

9 All right. Let's begin.

10 MR. RAIDER: And, Your Honor, just to introduce
11 myself as counsel for LabMD, I am Mr. Raider.

12 THE COURT: All right.

13 -- -- --

14 MICHAEL JOHN DAUGHERTY

15 being first duly sworn by the Courtroom Deputy Clerk,
16 testifies and says as follows:

17 -- -- --

18 DIRECT EXAMINATION

19 BY MR. RAIDER:

20 Q. Would you please state your name for the record?

21 A. Michael John Daugherty.

22 Q. What is your role at plaintiff LabMD?

23 A. I'm the founder and CEO of LabMD.

24 Q. How long have you been CEO of LabMD?

25 A. Since 1996.

1 Q. What services has LabMD offered?

2 A. We are a medical laboratory doing cancer detection,
3 tumor markers, bacterial detection in the urology
4 marketspace.

5 Q. What services are you currently offering?

6 A. Currently we are billing services for prior specimens
7 that were tested and access to medical records for the
8 physicians and -- physicians that need to still have access.

9 Q. And when did you stop offering cancer detection testing
10 services?

11 A. Our last specimen I believe was taken around the 9th of
12 January of 2014 and our last result was released around
13 January 15th, 2014.

14 Q. And what caused LabMD to stop offering cancer detection
15 services?

16 A. The overriding cloud and draining ongoing investigation
17 by the Federal Trade Commission.

18 Q. Could you turn to Tab 14 in your notebook?

19 A. Okay, I am in front of 14.

20 Q. And what is Exhibit 14?

21 A. 14 is the letter that I sent out to physicians,
22 administrators, nurses and support staff of our client base
23 on the 6th of January, 2014, letting them know we would no
24 longer be accepting specimens so that they could make
25 arrangements for other -- for their patients for future

1 medical testing.

2 Q. And if you would look at the third paragraph, could you
3 please explain the reasons you provided to your clients for
4 your business reason?

5 A. I said that FTC has subjected LabMD to years of
6 debilitating investigation and litigation regarding an
7 alleged patient information data security vulnerability
8 without standards, information or congressional approval and
9 without a consumer victim from the alleged breach, which is
10 in quotations.

11 The FTC has taken upon itself to spend your tax dollars
12 to ruin LabMD and regulate medical data security over and
13 above HIPAA.

14 THE COURT: And do you intend to introduce this?

15 MR. RAIDER: Yes.

16 THE COURT: Well, before you publish it, don't you
17 think you should do that?

18 MR. RAIDER: We were going to offer to tender the
19 exhibits at the end unless there was an objection made to the
20 exhibit.

21 THE COURT: Well, have you worked that out with the
22 FTC?

23 MR. RAIDER: We have not.

24 THE COURT: All right. Well, you probably
25 shouldn't publish anything until it's been introduced in

1 evidence, and basically that's what Mr. Daugherty has
2 done. So you can either see if there is an objection, and if
3 there is --

4 MS. FASCETT: There is no objection, Your Honor.

5 THE COURT: Then it's admitted. But you need to do
6 that for each of the exhibits.

7 MR. RAIDER: Okay. Thank you, Your Honor. We
8 will.

9 BY MR. RAIDER:

10 Q. Where are LabMD's records today?

11 A. LabMD's records are in the cooperate condominium and the
12 basement of my residence.

13 Q. What outside sources have access to your servers in the
14 condo?

15 A. There is a support volunteer that's helping who has had
16 years of experience in medical urology office space. He's
17 helping with the billing and winding down and answering
18 questions. And then myself.

19 Q. Is there remote access to the servers?

20 A. There is no remote access except to the billing
21 software. There is no remote access to any of the vast
22 majority of electronic records in the laboratory information
23 system.

24 Q. The FTC has issued a proposed order addressing LabMD's
25 future conduct. What are the obligations the FTC has

1 proposed to be imposed against LabMD?

2 A. They wanted a consent decree that wanted twenty years of
3 biannual audits from an outside source at our expense. It
4 would also open us up to additional penalties and/or fines.

5 MR. GORJI: Your Honor, I'm going to object. It's
6 not something that -- negotiations are not something that
7 would be held against the FTC at this point. There is an
8 administrative complaint that's been filed, but a consent
9 decree is a negotiation.

10 THE COURT: Well, have you offered -- have you
11 shown them a consent decree with a proposal that that would
12 resolve the matter?

13 MR. GORJI: There have been negotiations,
14 Your Honor, in the past.

15 THE COURT: Well, is it -- would the FTC ever agree
16 not to resolve this case without an ongoing consent decree
17 subjecting them to monitoring over a long period of time,
18 which is my experience with the FTC?

19 MR. GORJI: Your Honor, my understanding is that
20 negotiations are no longer occurring. There is an
21 administrative complaint and an ongoing administrative
22 process that doesn't necessarily request the exact same
23 relief.

24 THE COURT: Well, you can cross-examine him on
25 that, and once the cross-examination is done, I will

1 determine whether or not that's something that would go into
2 my consideration.

3 MR. GORJI: Sure, Your Honor.

4 Your Honor, if I may? I plan on handling the
5 cross-examination, Ms. Fascett plans on handling the argument
6 today, if that's all right with the Court?

7 THE COURT: That's fine.

8 MR. GORJI: Thank you.

9 BY MR. RAIDER:

10 Q. Is it your understanding that the fact that LabMD is
11 merely archiving its records today would change the relief
12 the FTC is seeking against LabMD?

13 A. No, it's not. That's not my understanding.

14 Q. Let's go back a step and discuss LabMD when it was
15 providing cancer detection services in 2013 and the years
16 before.

17 How much revenue did LabMD generate each year roughly?

18 A. It ranged between three and a half to seven and a half
19 to eight million approximately.

20 Q. And how much revenue has LabMD generated in calendar
21 year 2014?

22 A. Approximately fifty thousand dollars.

23 Q. And how much revenue has LabMD projected to generate in
24 the second half of 2014?

25 A. Probably another fifty to seventy-five thousand

1 dollars.

2 Q. And how much profit did LabMD generate in the years it
3 was generating millions of dollars in revenue?

4 A. With the exception of 2013, our profit margin was
5 approximately 25 percent. In 2013 we lost approximately half
6 a million dollars.

7 Q. How much profit has LabMD generated so far in calendar
8 year 2014?

9 A. None.

10 Q. And looking to the second half of calendar year 2014,
11 how much profit is LabMD expected to generate?

12 A. Zero.

13 Q. How many employees did LabMD have on its payroll in
14 2013?

15 A. Between 25 and 30.

16 Q. And how many employees does LabMD have today?

17 A. One.

18 Q. I want to shift topics again and talk a little bit about
19 LabMD's insurance program.

20 A. Okay.

21 Q. What types of insurance did LabMD have when it was
22 offering cancer detection services?

23 A. We had medical malpractice for the company, we had
24 malpractice for the physicians, we had directors and officers
25 insurance, we had general liability insurance, we had medical

1 insurance, dental insurance, workmen's comp and vision.

2 I think that's everything.

3 Q. Which of these policies does LabMD currently have?

4 A. We have a COBRA for medical and dental, and that is
5 all.

6 Q. In the years 2013 and before, what issues did LabMD
7 encounter in obtaining insurance?

8 A. We never had problems getting insurance prior to 2013.

9 Q. Were you told why your insurance -- why LabMD's
10 insurance policies would not be renewed?

11 A. Yes. Because of the -- the claims that weren't renewed,
12 is was because of the FTC investigation, the ongoing cloud,
13 and the fact that it involved medical records. So that even
14 the policy that wasn't even covering a claim of that type was
15 refused for that reason, meaning the medical malpractice
16 insurance.

17 Q. And let me refer you to Exhibit 15 in your notebook.

18 A. Yes.

19 Q. And let me ask you some --

20 MR. RAIDER: Your Honor, I would like to show this
21 to the witness and establish a foundation.

22 BY MR. RAIDER:

23 Q. What is this document?

24 A. This is an e-mail string from our broker that was sent
25 to me between I believe our broker and one of his staff

1 members and an underwriter for OneBeacon Pro.

2 Q. And how did you receive a copy of this?

3 A. Because the broker sent it to me to show me that the
4 company wasn't going to be interested in insuring --

5 MR. GORJI: Objection, Your Honor. Hearsay.

6 THE COURT: Is there any objection to this e-mail?

7 MR. GORJI: Your Honor, I can get into it on cross.

8 THE COURT: Pardon me?

9 MR. GORJI: I can get into it on cross.

10 THE COURT: So is there any objection to the
11 introduction of the e-mail?

12 MR. GORJI: No, Your Honor.

13 THE COURT: It's admitted.

14 BY MR. RAIDER:

15 Q. Who is Mr. Coscarelli?

16 A. Mr. Coscarelli is an underwriter at OneBeacon Pro who
17 communicated with my broker.

18 Q. Who is Mr. Seilkop?

19 A. Fred Seilkop is the owner of -- I believe of Healthcare
20 Professional Services and my broker.

21 Q. And who is Ms. Garrido?

22 A. Betsy Garrido is an assistant that works for Mr. Seilkop
23 at Healthcare Professional Services.

24 Q. What insurance policies are being discussed in this
25 e-mail thread?

1 A. This is the facility, what we call tail coverage or ERP,
2 which is extended reporting period coverage. After a
3 practitioner, a medical facility, ceases practicing their
4 operations in that manner, then you have to get coverage to
5 extend any claims that come for that reporting period where
6 they were working there.

7 Q. What reason is Mr. Coscarelli offering for declining to
8 offer insurance to LabMD?

9 A. He says, The potential volatility due to the FTC
10 investigation is something we want to stay away from,
11 particularly because it pertains to medical records.

12 Q. Has LabMD been able to obtain an offer for an extended
13 reporting period after January 2014?

14 A. I split the search. We had almost everyone say no.

15 I did have -- I found a company in Florida who offered
16 tail coverage to the physicians, so I split them off and got
17 their own tail coverage, and we don't have any medical
18 coverage, medical malpractice coverage.

19 Q. You mentioned having comprehensive general liability
20 insurance. What is the status of your efforts to renew that
21 policy?

22 A. They nonrenewed effective May 5th of this year -- that
23 was Hartford -- because of the Federal Trade Commission
24 claims history.

25 Q. And what impact does that have on LabMD's ability to

1 offer cancer detection services?

2 A. Well, to offer cancer detection services, you obviously
3 have to have a facility where you can offer that, and we are
4 required to have general liability insurance in our facility
5 and under our lease or anywhere else where we want to open up
6 space.

7 So without being able to get general liability
8 insurance, we can't function.

9 Q. I want to switch topics again and talk a little bit
10 about the regulatory oversight of LabMD as an ongoing
11 provider of cancer detection services.

12 Separate from the FTC, was LabMD subject to government
13 regulation?

14 A. Yes.

15 Q. By whom?

16 A. By the federal -- the U.S. government and the State of
17 Georgia under CLIA and DHR has a -- there is a laboratory
18 oversight group within the Department of Human Resources in
19 the State of Georgia.

20 Q. And in years 2013 and before, how many times has HHS
21 raised concerns about LabMD's compliance with HHS
22 regulations?

23 A. We never had a problem.

24 Q. And what about as to the State of Georgia?

25 A. No, no problems.

1 Q. If you could turn to Exhibit 23 in your notebook?

2 A. Okay.

3 Q. What is this document, just at a high level so we can
4 get it introduced into evidence?

5 A. It is a -- we are required to submit specimens to an
6 independent source that reports to the government our testing
7 and accuracy, and so that's what that is.

8 Q. Is this a business record of LabMD?

9 A. Yes, it is.

10 MR. RAIDER: We tender this into evidence,
11 Your Honor.

12 THE COURT: Any objection?

13 MR. GORJI: No objection, Your Honor.

14 THE COURT: It's admitted.

15 BY MR. RAIDER:

16 Q. What does it mean to have a rating of 100 percent
17 compliance?

18 A. That means that all the tests came within 100 percent of
19 the acceptable range of the independent agency on the
20 testing -- on the results we reported. So it's an accuracy
21 of test reporting reports.

22 Q. The certificate indicates a November 2013 expiration
23 date. What was the status as of January 2014?

24 A. I'm sorry, can you point the certificate out? I'm not
25 seeing it.

1 Are you on 23?

2 Q. Yes. I'm looking at the --

3 A. I'm on a different 23.

4 Q. -- expiration date on the right?

5 A. My 23 is not the same as your 23.

6 THE WITNESS: Can he show me --

7 THE COURT: This is not my hearing. This is your
8 lawyer's.

9 THE WITNESS: Okay. That's my 23.

10 THE COURT: Why don't we do this. Since you have
11 three other lawyers here with you, maybe they could find this
12 for you and we can move on.

13 MR. RAIDER: Okay, we will.

14 MR. GORJI: Your Honor, I would also like to make
15 sure the government has the correct 23 as well.

16 MR. RAIDER: Yes. I apologize for that.

17 THE COURT: My understanding is that Exhibit 23 is
18 a one-page document that is sent by the American Proficiency
19 Institute and it's dated March 5th of 2014.

20 MR. RAIDER: Yes.

21 THE COURT: Is that Exhibit 23?

22 THE WITNESS: No.

23 MR. RAIDER: That's what we are asking to have
24 admitted.

25 THE COURT: Well, that one-page document has been

1 admitted.

2 MR. RAIDER: Yes. And I will move on.

3 BY MR. RAIDER:

4 Q. You said that HHS has not raised any concerns about
5 LabMD's compliance with HHS regulations. What issues
6 specifically, if any, has HHS raised concerning LabMD's data
7 security program?

8 A. None.

9 Q. Has HHS launched an enforcement action against LabMD
10 because of concerns over its data security program?

11 A. No.

12 Q. Have they, to your knowledge, instituted an
13 investigation?

14 A. No.

15 Q. Have they issued notices of violation or documents to
16 that effect?

17 A. No, sir.

18 Q. Okay. I want to switch topics one more time and talk
19 about your website and your blog.

20 Have you created a blog?

21 A. Yes.

22 Q. And what is the website that hosts that blog?

23 A. *MichaelJDaugherty.com*.

24 Q. And on your blog, have you posted opinions about the
25 FTC?

1 A. Yes, I have.

2 Q. And could you describe what you have said about the
3 FTC?

4 A. I have -- I'm very opinionated about the overreach and
5 lack of standards for rules or clarification and yet still
6 the exhaustive investigation. So I have posted what
7 I consider to be my opinion and First Amendment right
8 speech about how they have conducted themselves throughout
9 this.

10 Because we have never known what we have done wrong, and
11 that's been a huge frustration, and it's so damaged the
12 organization that I have spoken about that in several blogs.

13 Q. In your dealings with FTC employees as part of this
14 LabMD enforcement action, what did you perceive to be the
15 reaction to your blog posts criticizing the FTC?

16 A. My perception is that they are very upset and unhappy
17 about it. They don't like any public criticism.

18 Q. Is it your opinion that the FTC has retaliated against
19 LabMD because of your blog criticizing the FTC?

20 MR. GORJI: Objection.

21 THE COURT: Overruled.

22 A. Yes, it's my opinion that they retaliated.

23 Q. Has the FTC monitored your website with the blogs?

24 A. Yes, they have.

25 Q. Okay. I want to discuss Google Analytics. What is

1 Google Analytics?

2 A. Google Analytics is a tool provided by Google to analyze
3 the traffic and effectiveness of --

4 MR. GORJI: Objection, Your Honor, to the basis for
5 his knowledge. There is no foundation here. He does not
6 work for Google.

7 The attachments that he's provided to his
8 declarations he has no basis for authenticating. We are
9 objecting on those grounds, Your Honor.

10 THE COURT: Are you denying that the FTC has
11 monitored his blog?

12 MR. GORJI: No, I'm not denying that. But,
13 Your Honor, the specificity of representations made in the
14 declaration have no foundation.

15 THE COURT: All right. Well, maybe we could bring
16 somebody in from Google and extend this hearing, if you would
17 like.

18 It seems odd that if you are an enforcement
19 regulatory body, that rather than doing your regulatory
20 activity, that you would be monitoring somebody's blog that
21 is criticizing the FTC, unless you are thin-skinned about
22 that.

23 MR. GORJI: Your Honor --

24 THE COURT: You have just acknowledged that the FTC
25 is monitoring his blog. Are you doing that in connection

1 with your regulatory investigation or are you doing that for
2 your interest in his company and what they are saying about
3 it, about the FTC?

4 MR. GORJI: Your Honor, the government and agencies
5 monitor individuals' websites on a routine basis. In
6 addition, here, Your Honor --

7 THE COURT: Why?

8 MR. GORJI: To determine whether or not there is
9 any information that they might be able to add to their
10 case.

11 THE COURT: So are you doing that in connection
12 with your regulatory activities and responsibilities in
13 connection with this investigation of LabMD?

14 MR. GORJI: Your Honor, I would have to confer with
15 the FTC officials on the exact reason. I haven't been
16 provided an exact reason.

17 And, again, the suggestion that it's for
18 retaliatory purposes is purely speculative. There hasn't
19 been any --

20 THE COURT: Well, under the Federal Rules of
21 Evidence, somebody who has an experience that would provide a
22 foundation for an opinion is admissible as a lay opinion.

23 He has now gone through this investigation
24 beginning with the FTC's investigative activity beginning in
25 2010, which is now four years ago, and it would seem to me

1 that if he is able to establish when he began these public
2 criticisms of the FTC and compare that with the investigative
3 activity of the FTC and its various responses to actions that
4 he's taken, that he could reach an opinion about whether or
5 not he believed it to be or that it was his opinion that they
6 were acting in a retaliatory manner, and, therefore, I'm
7 going to overrule the objection.

8 MR. RAIDER: Your Honor, as to the specific
9 reports, I just want to make clear that those also, I mean,
10 if we establish a foundation, they would be admissible at
11 this point. Is that part of your --

12 THE COURT: Probably not through him.

13 MR. RAIDER: Well, we would argue under Federal
14 Rule 807 that there is sufficient reliability, that this is a
15 service Google makes available to website owners to pull down
16 information about traffic on their website.

17 THE COURT: Yeah, but the question would be the
18 reliability of the information being provided by Google, and
19 I don't think he has a basis to express that opinion.

20 MR. RAIDER: Understood, Your Honor.

21 BY MR. RAIDER:

22 Q. Just to go back and make sure, what is Google
23 Analytics?

24 A. Google Analytics is a service or/and a tool that Google
25 provides to website users, owners, to analyze and pull

1 reports down from Google's data of who is looking at the
2 website, how long they stay, how deep they go, who they are,
3 and so you can -- as a website owner, you can assess the
4 effectiveness of reaching the audience you want to reach and
5 you can see what audience you are pulling in.

6 Q. Have you generated website visit reports for your web --
7 for your blog post website?

8 A. I have, yes.

9 Q. What type of reports did you generate?

10 A. I generated the reports that would show who the top
11 users were and what dates they were on and what ranges, and
12 coincided those to some blog posts.

13 Q. What type of blog posts were you focusing on?

14 A. Well, as an example, there was a blog post when I first
15 really announced that the FTC was suing me, which came out
16 approximately September 17th, 2012.

17 And while I noted the Federal Trade Commission up until
18 September 1, 2012, had never looked at my site one time, on
19 that day or approximately that day or the day after the
20 Federal Trade Commission had looked at that blog 75 times.

21 MR. GORJI: Objection, Your Honor. Again, there is
22 no reliability for this testimony.

23 THE COURT: Is that true, that after this blog
24 post, that there were 75 hits by the FTC in response to his
25 criticism?

1 MR. GORJI: I don't know the answer to that,
2 Your Honor. I haven't --

3 THE COURT: Will you find that out for me? Will
4 you?

5 MR. GORJI: Your Honor --

6 THE COURT: Will you find that out for me?

7 MR. GORJI: I could contact Google and have FTC
8 experts --

9 THE COURT: Why don't you contact your agency and
10 find out if anybody in response to a critical blog post 75
11 times the next day accessed the blog?

12 MR. GORJI: Well, Your Honor --

13 THE COURT: And explain to me what was on the blog
14 post that was of interest to your investigation of this
15 company.

16 MR. GORJI: Your Honor, one --

17 THE COURT: Will you do that?

18 MR. GORJI: I can have FTC provide an explanation
19 for that.

20 Your Honor, one aspect of this case is that there
21 is retaliation, and in order to demonstrate retaliation,
22 there has to be that his freedom of speech has been adversely
23 affected. So it would make sense, Your Honor, for the
24 government to continue to monitor whether or not he's still
25 continuing to express his speech.

1 And I believe he is still effectively expressing
2 his speech, and, therefore, there is a legitimate reason.

3 THE COURT: Are you telling me as an officer of the
4 court that after a critical blog post, that somebody at the
5 FTC, in order to make sure that he was -- that he was not
6 impeded in his First Amendment rights, decided the next day
7 to 75 times make sure that the same post was up there and,
8 therefore, it could come in and make an argument like you
9 have just made, that the purpose of that access was to make
10 sure that he was unimpeded in the exercise of his First
11 Amendment rights?

12 MR. GORJI: Your Honor --

13 THE COURT: Is that what you are saying?

14 MR. GORJI: Your Honor, that is not the sole
15 explanation.

16 THE COURT: Is that what -- is that one of your
17 explanations?

18 MR. GORJI: I believe that is a legitimate reason
19 for --

20 THE COURT: And is that why the -- is that why you
21 are representing to me that the FTC accessed his blog, was to
22 make sure that his First Amendment rights were not being
23 impeded?

24 MR. GORJI: No, I'm not making that representation,
25 Your Honor, that that is the sole reason.

1 THE COURT: So you are backing from what you just
2 told me?

3 MR. GORJI: No, no, Your Honor. I believe that one
4 legitimate basis for --

5 THE COURT: Was that a legitimate basis on behalf
6 of your client, the FTC, the reason why they accessed the
7 blog post 75 times the day after the post was made?

8 MR. GORJI: Your Honor, I would have to get FTC to
9 provide an explanation as to why they accessed it. I can --

10 THE COURT: You just told me twice that's one of
11 the reasons they accessed it. Is that one of the reasons why
12 they accessed it?

13 MR. GORJI: Well, Your Honor, I know that's one of
14 the reasons why I accessed it, for example, during the course
15 of this litigation.

16 THE COURT: Did you access it on September 17th or
17 September 18th?

18 MR. GORJI: No, Your Honor.

19 THE COURT: How many times have you accessed it?

20 MR. GORJI: Maybe a handful, Your Honor. But --
21 and that was my motivation.

22 But I can also surmise, Your Honor, that a
23 government agency might think that there is possibility of
24 statements related to the conduct -- to the conduct that FTC
25 is trying to regulate on his postings and looking for that

1 reason.

2 Now, whether or not that is the actual motivation
3 here, Your Honor, I can't attest to that. I can ask FTC to
4 provide you with their explanation.

5 THE COURT: This is taking an interesting and
6 troubling turn which I never expected, for an admission by an
7 FTC lawyer that they monitor blogs routinely of companies for
8 whatever purposes, and you don't even know the purposes
9 except for this purpose, that the only purpose that you have
10 expressed, which I find incredible, is that you stated on
11 behalf of your agency that the day after this blog posting
12 was made, that the 75 times -- assuming that's true, but even
13 if it was seven times, that they monitored it to make sure
14 that his First Amendment rights were not being impeded, is
15 incredible.

16 MR. GORJI: Your Honor, that's not my sole
17 explanation. My other explanation --

18 THE COURT: But it's one of your explanations,
19 isn't it?

20 MR. GORJI: Your Honor --

21 THE COURT: Isn't it?

22 MR. GORJI: Your Honor, I think perhaps that is
23 probably an explanation as to why I personally did it. With
24 respect to the FTC, I don't know whether or not that
25 motivated --

1 THE COURT: Was my question unclear about the
2 accessing of the website the day after the posting? Did you
3 not understand that?

4 MR. GORJI: Your Honor, your question was
5 not unclear. I perhaps was confused, but not because of the
6 lack of clarity of your question. I apologize to the
7 Court.

8 Again, I can have the FTC provide an explanation as
9 to why they are monitoring, and my explanation is again what
10 I surmise, but it may not be sufficient here. And,
11 Your Honor, if Your Honor would like, we could have FTC
12 provide an explanation to the Court.

13 THE COURT: Well, let's have this rule between you
14 and me at least. This is a hearing. I am a judicial
15 officer, and you are an officer of the court. When I ask you
16 a question, don't duck and cover the question. Answer the
17 question so that I know that what you are telling me is
18 accurate and I can rely upon it. Is that fair?

19 MR. GORJI: That's fair, Your Honor. I didn't
20 intend to give the impression that I knew what the reason
21 was. I was providing an explanation as to why I think it
22 might be reasonable.

23 THE COURT: Well, that's not what you said, and the
24 record will be clear that in answer to my two questions, that
25 is not what you said.

1 MR. GORJI: I apologize.

2 THE COURT: Instead you were coming up with a
3 defense for the conduct. And that's a problem that lawyers
4 have when they are unarmed with the facts.

5 MR. GORJI: I agree, Your Honor, I do not have the
6 facts with respect to what their specific reasoning was.

7 THE COURT: Then the next time you answer a
8 question, tell me that.

9 MR. GORJI: I apologize that I gave a misimpression
10 to the Court, Your Honor.

11 THE COURT: Well, that's not a misimpression. You
12 apologized for making an inaccurate statement in response to
13 a question from the bench.

14 MR. GORJI: I apologize, Your Honor.

15 THE COURT: Thank you.

16 BY MR. RAIDER:

17 Q. Mr. Daugherty, if you could turn to Tab 31. Hopefully
18 these numbers are correct.

19 A. I'm at 31, sir.

20 Q. Are those the Google Analytic reports that you
21 generated?

22 A. Let me just review them, please.

23 Yes, sir. I believe those are all of them, yes, sir.

24 Q. And did you generate those reports?

25 A. Yes, I did.

1 Q. And how did you go about generating those reports?

2 A. I just signed onto my account or my password and ID
3 that's hooked up to the website and started using the tool.

4 Q. I want to turn to the report. And I have the single
5 pages in my notebook, unfortunately. I'm not sure how far
6 into the exhibit it is. January 1 --

7 MR. RAIDER: Well, Your Honor, we tendered these
8 reports for Mr. Daugherty to explain the information on them
9 that he received.

10 THE COURT: So what does that mean, tendered to
11 what?

12 MR. RAIDER: We would like to admit these reports
13 into evidence.

14 THE COURT: Any objection?

15 MR. GORJI: Again, Your Honor, the government
16 objects based on reliability.

17 THE COURT: Sustained.

18 BY MR. RAIDER:

19 Q. Was there information posted to your blog website that
20 would shed light on the adequacy of LabMD's data security
21 practices?

22 A. No, sir.

23 Q. Were you surprised by the number of times the FTC
24 visited your website?

25 A. Very.

1 Q. Was there any reason that you are aware of why the FTC
2 employees would have to view your blog website so many
3 times?

4 A. As involved the investigation, no.

5 Q. I want to switch topics one last time. What is LabMD
6 asking from the Court?

7 A. We are asking the Court to stop or pause the
8 investigation so that we can try to recover from the cloud
9 and loss of business revenue and loss of employees and loss
10 of insurance and loss of reputation and revenue and we can
11 try to start to recover.

12 Since they don't have standards and rules and won't tell
13 us what we have done, they just point to consent decrees that
14 say no wrongdoings in them and we have -- we just have --
15 it's been ongoing for years of not knowing what we are
16 supposed to do or what we did wrong, and we have just been
17 torpedoed.

18 Q. If the Court were to stop the FTC's enforcement
19 proceedings against LabMD, would you restart the business to
20 begin offering cancer detection testing services?

21 A. It would -- I would start the attempt to. We can't get
22 insurance with this over our head. That's the first thing.
23 And we have to -- and we are also being sued by the
24 landlord. So we have a long stretch to get back.

25 And our key employees have left to other labs. Our

1 clients have left to other labs. Our landlord is suing us
2 because we had to leave the lease earlier -- early.
3 We have -- the insurance is not there.

4 And all that healing has to happen. So that will be
5 able to start that, and also prevent us from going deeper in
6 the hole by having no longer -- no longer having access for
7 the physicians for the records they need now, which are
8 required by us to keep, depending on the record, from five to
9 ten years.

10 MR. RAIDER: Thank you, Mr. Daugherty. I have no
11 further questions.

12 THE COURT: All right. Cross?

13 MR. GORJI: Yes, Your Honor.

14 -- -- --

15 CROSS-EXAMINATION

16 BY MR. GORJI:

17 Q. Good morning, Mr. Daugherty. How are you?

18 A. Good morning.

19 Q. I have got a question about the investigation and your
20 speech. You agree that the investigation was already
21 underway before you started criticizing the FTC's conduct
22 here?

23 A. Well, in January of 2010 they started a nonpublic
24 inquiry. If you consider that an investigation, yes.

25 Q. And you began your criticism in early 2012; is that

1 correct?

2 A. My public criticism?

3 Q. Yes, your public criticism.

4 A. That was my blog. Yeah, I think the public criticism
5 started with the *Atlanta Business Chronicle* interviewing me,
6 and I believe that came out in September approximately 7th of
7 2012.

8 And that was because I had to do it because the Federal
9 Trade Commission had filed suit for me to -- let me think.
10 Let me just think here.

11 I mean, in August of '12, I believe that's when they
12 sued for the CID, and that's when people started noticing and
13 contacting me. Up until that point no one had known and
14 I hadn't told anyone. But I was really forced to respond at
15 that point.

16 Q. And your understanding is that the company Triversa
17 found information about your patients, your customers? That
18 was in 2008, is that correct, that you learned of Triversa
19 finding that information?

20 A. Tiversa was contacted -- contacted me or my company
21 LabMD in May of 2008.

22 Q. And the CID, the subpoena for information and documents
23 from FTC to your company, that was in December 2011; is that
24 right?

25 A. I'm sorry, yeah. You know, that's why my memory -- I

1 believe they filed the CID in December of 2011, and then the
2 Department of Justice filed in August of 2012 to have the
3 Court decide whether I had to sit for a CID.

4 Q. So your public criticisms began well after the CID was
5 served on the company; is that right?

6 A. Well, it didn't -- the CID service from 2012 -- 2011, I,
7 believe that was. Okay, I'm getting my years mixed up. Yes,
8 yes.

9 So '11 they served right at Christmas, and no one picked
10 it up publicly. And then when the DOJ I believe filed to
11 have the Court decide whether I was required to, that's when
12 the public started to come to me. That was the first
13 time. So that's --

14 Q. So just so we are clear, and without focusing on dates,
15 the CID came first, and then you started publicly
16 criticizing?

17 A. Yeah, the CID -- I mean, yeah, the CID came in December
18 23rd, 2011, and the criticism was in September 2012.

19 Q. During the course of that time frame, between the CID
20 coming and your public criticism, were there any depositions
21 that took place with respect to employees of your company?
22 Were there any other investigative things that occurred that
23 impacted your company before you started publicly
24 criticizing?

25 A. Well, yeah. The Federal Trade Commission was repeatedly

1 demanding more and more and more and more information,
2 totally side-swiping my management team. Because we were in
3 a house of mirrors, never-never land, not knowing what they
4 wanted, and they wouldn't tell us what we did wrong, and it
5 was relentless.

6 So it was -- and you are talking a company of like
7 thirty people that diagnose cancer with one VP of
8 operations.

9 Q. So the FTC was actively investigating before you started
10 your public criticism?

11 A. Yes.

12 Q. I want to draw your attention to the FTC administrative
13 complaint. Have you had a chance to look at that document?

14 A. Can you refresh my memory or bring it to me, please?

15 MR. GORJI: One moment, Your Honor.

16 THE WITNESS: I assume I can close this?

17 MR. GORJI: You should have it --

18 THE WITNESS: Oh, it's in the book?

19 MR. GORJI: You should have it as your Exhibit 8.

20 THE WITNESS: Okay.

21 BY MR. GORJI:

22 Q. Okay. Are you familiar with this document?

23 A. Yes, sir, I am.

24 Q. Okay. To date, has the FTC ordered you to do anything
25 that would change your business conduct with respect to

1 managing patient-protected information?

2 A. No.

3 Q. Now, in your verified complaint in your declaration, you
4 say that the cause of your company having to essentially wind
5 down its business is a result of the FTC investigation?

6 A. That's correct.

7 Q. But it's not a result of anything that FTC has actually
8 ordered you to do with respect to how to manage your
9 patients', customers' protected information, is it?

10 A. We would have liked to have known that long ago. No, we
11 haven't gotten that answer.

12 Q. Would you say that that is the primary reason why?

13 A. Yes.

14 Q. Have you ever given a contrary reason as to why your
15 company had to wind down?

16 A. Contrary?

17 Q. Yes.

18 A. I have given additional. I wouldn't say contrary.

19 Q. What reason would you say?

20 A. I said that the Federal Trade Commission set the stage
21 for our having to wind down operations because as a small
22 company this was an overarching fishing expedition that never
23 gave us standards, rules, reasons, and that just unspeakably
24 slowed down a cancer detection center.

25 Because we only have so much energy, and so we had to

1 focus on this, and the only answers we were getting back was
2 look at this consent decree, which was vague at best with
3 fine print about no wrongdoing is admitted.

4 So we were in a never-never land. So we had to shoot --
5 we don't know where we had to shoot, so we felt the only way
6 to get in a safe place would be to shoot for perfection.

7 So I had, you know, the management staff, especially the
8 IT and my VP of operations, just spending so much time on
9 that, and that energy was taken away from prepping for what
10 we knew what was coming, which was Obamacare.

11 And so when we had plans to go into molecular science or
12 into breast pathology, we couldn't get off the ground because
13 we were getting diverted over here.

14 Because as a cancer detection center in a niche market,
15 you specialize in just one area, and the expertise is just --
16 or the differentiation in the market is our expertise by our
17 pathologists because they just read that kind of cancer, and
18 that is something that physicians around the country want and
19 patients benefit from, because practice makes perfect.

20 With Obamacare it was coming that that priority was
21 fading away, and we were aware of that, and we were going to
22 have to diversify our base.

23 And the Federal Trade Commission tied our feet
24 together. We only have so much energy and time, and it was
25 just overpounding for this small company.

1 So I have said several times that the Federal Trade
2 Commission set the stage during this time so that we could
3 not function and deal with what came with Obamacare.

4 And then with four weeks' notice due to sequestration,
5 which usually it's more, we found out that our 2013
6 reimbursement was cut 30-something percent for pathology, and
7 we started bleeding cash like crazy. And we were just so
8 overwhelmed. It was like too many spinning plates.

9 And so -- and then that's just -- that's just the
10 business model. Then you go into the specific knowledge that
11 the VP of operations especially had and the IT guys, and
12 really just how the fear and the unknown and the uncertainty,
13 and eventually it just wore them down, and my VP left and he
14 moved to Denver in August. And when that happened, that was
15 just it.

16 And so we started losing, losing money. And then by --
17 I didn't want to ruin everyone's Christmas, but around
18 December I knew this is just not looking good. It was just
19 reality. We just were overwhelmed with reality.

20 So the FTC is not going away, we are not going to get
21 more money, our reputation has been hashed, people that are
22 employees are just afraid and so they are just leaving.
23 And I couldn't give answers.

24 And so, you know, the ship just went down.

25 Q. Well, how would you say Obamacare itself impacted your

1 business?

2 A. Because CMS starts cutting costs for costs containment,
3 and ancillary services went first. And so, you know, for
4 cost containment those fee schedules were cut.

5 Q. And how about customers that you previously had, were
6 they going to be referred to you for services under
7 Obamacare?

8 A. Well, no, because what happened was what Obamacare does
9 is it really forces a marketplace consolidation, and so
10 physicians in the short term to survive were going to have
11 to -- the physicians that we had -- I mean, this is not all
12 physicians, period. I mean, this is just urologists and
13 office-based urologists. So that's another reason why we've
14 got to diversify.

15 But they were forced to either -- they either get huge
16 and merge together, they either sell their practice to
17 hospitals, or they retire.

18 And so we saw people having to basically survive for a
19 consolidation reason, and so the purchasing -- you know, we
20 knew that physicians were going to have to have economies of
21 scale, so we were going to have to broaden who our customers
22 could be to be able to get enough customers to survive
23 because reimbursement was going down.

24 Q. So as a result of Obamacare, you lost a considerable
25 amount of business?

1 A. No, we didn't -- well, we didn't lose business. We lost
2 the revenue for the business we performed, and we were
3 prevented because of the FTC action from building the
4 business to survive. We could only handle one tidal wave at
5 a time. We had two coming at us.

6 Q. Well, isn't it true that physicians and customers were
7 not -- under Obamacare were no longer going to be able to
8 refer to you for services?

9 A. In the urology marketplace, no.

10 MR. GORJI: One moment, Your Honor.

11 Your Honor, at this time I would like to
12 cross-examine Mr. Daugherty with material that comes from the
13 FTC administrative proceedings. It involves a deposition
14 transcript.

15 Under FTC regulations it is protected and
16 confidential, but there is a provision under the regulations
17 that allows for its disclosure provided that we give
18 notice. We did so last week, Your Honor.

19 But because it was previously confidential, I would
20 like to give counsel an opportunity to take whatever measures
21 they think necessary before I present it in open court.

22 THE COURT: And is this related to his direct
23 testimony?

24 MR. GORJI: Your Honor, it addresses specifically
25 whether or not Obamacare was the cause of loss of revenue and

1 the winding down of the company.

2 THE COURT: It is being offered as a prior
3 inconsistent statement?

4 MR. GORJI: Yes, Your Honor.

5 THE COURT: So, Mr. Raider, what do you say about
6 that?

7 MR. RAIDER: Your Honor, we would ask that a
8 protective order apply and it be sealed at least for now
9 until we see where it's going consistent with its status in
10 the administrative proceeding.

11 THE COURT: I mean, can you introduce as a prior
12 inconsistent statement a statement that you elicited in his
13 examination?

14 Because he didn't say anything about Obamacare on
15 direct examination. So you elicited the explanation on cross
16 regarding Obamacare, and now you want to impeach the
17 statement that you elicited with a prior inconsistent
18 statement? And if so, how can you do that?

19 MR. GORJI: Well, Your Honor, he testified on
20 direct that FTC's actions are the reason why his company had
21 to wind down.

22 I asked him here whether or not he believes
23 Obamacare is what caused it, and he says no, but I would like
24 to point him to his testimony where he says the opposite in a
25 deposition, sworn statement.

1 THE COURT: I know, but it's still testimony that
2 you elicited on cross, and now you want to -- can you offer a
3 prior inconsistent statement to rebut a statement that you
4 elicited?

5 MR. GORJI: Your Honor, I think I can impeach him
6 if he says something that's inaccurate. I can't bring in
7 rebuttal evidence, bring somebody else in to impeach him, but
8 I have a deposition, a sworn deposition.

9 THE COURT: Right. So what's your authority for
10 that? Since you have been laying in wait to do this, so you
11 must have a case or two for me to support the admissibility
12 of --

13 MR. GORJI: Your Honor, I do not have any case law
14 with me, and I wasn't at this moment seeking to introduce the
15 exhibit. I was simply seeking to make use of it in open
16 court to contradict the testimony here.

17 THE COURT: And do you have any authority that this
18 protected material that I assume you got through this
19 deposition under these circumstances should be allowed?

20 MR. GORJI: Your Honor, there is a provision, a
21 regulation, 16 CFR Section 410 (g), that allows for its use
22 upon notice to the party who has given the testimony in the
23 deposition.

24 THE COURT: Of course, nobody ever told me you had
25 done that. I had no idea this was coming up. I would like

1 to say I'm a pretty diligent fellow, but because nobody told
2 me about these regulations, I will admit I haven't gone to
3 look at them and I haven't memorized them.

4 So I do like to make careful rulings, and, you
5 know, maybe there is another way of doing this, that you
6 could submit after the hearing those portions that you claim
7 are prior inconsistent statements, and the lawyer for LabMD
8 can weigh in on whether or not it is or not, and then I can
9 consider it after that.

10 But it seems to me fundamentally unfair that, one,
11 you knew this was coming; two, you don't have any authority
12 for me; and that you now want to disclose because you have
13 given notice in this very public setting something which
14 I think you know is not going to be favorable to this man
15 individually and reputationally and in the lawsuit.

16 MR. GORJI: Your Honor, we did provide notice last
17 week that we were going to make use of this transcript, so it
18 wasn't trying to ambush anybody here.

19 THE COURT: Well, make use of it? Did you tell
20 them in what specific way?

21 MR. GORJI: Actually, our filing from last week
22 indicated that it would be to cross-examine him.

23 THE COURT: For whatever happens to be in that,
24 without focusing on specifically what it is that you were
25 going to use it for?

1 MR. GORJI: Well, we didn't identify the specific
2 topic.

3 THE COURT: But you knew that's the topic that you
4 were going to use, didn't you?

5 MR. GORJI: Yes, Your Honor.

6 THE COURT: Did you even have a communication with
7 opposing counsel to say, look, this is why we want to use it,
8 we don't -- our contention is that there were various and
9 sundry reasons why the business failed, and we have this and
10 you were there, and I just want you to know with respect to
11 this notice that that's the purpose?

12 MR. GORJI: Your Honor, I didn't believe that
13 providing an additional layer of specificity as to exactly
14 what from the transcript we were planning on using was
15 something that was necessary, and in light of the fact that
16 we told them we were planning on using it and that would
17 alert them as to whether or not their confidentiality
18 interests were going to be implicated, the use of the
19 transcript or not, not what the specific content of what I
20 was about to say in court would implicate --

21 THE COURT: Let me just make this observation.
22 There is a lot of acrimony in this case, and that impedes the
23 sort of professionalism that I expect at a hearing that
24 allows me to make a decision on a motion. I believe that
25 that is impeding and affecting your judgments as to the

1 fairness of this hearing.

2 And, you know, I preside over very difficult
3 criminal cases all the time where people's liberty is at
4 stake, and I find more cooperation between lawyers in those
5 on much more difficult issues, including evidentiary issues,
6 than I see in this proceeding, which is the government coming
7 in, which -- and I think it's the responsibility of the
8 government to be fundamentally fair to the people that it's
9 regulating, and that it would be in your interest and I would
10 hope your motivation as an employee of the government to say
11 here is what -- here is our position, here is how we are
12 going to advocate it, because we want the Judge to have a
13 clean record to make a decision.

14 So your explanation that you didn't think the
15 additional level of specificity may be technically correct --
16 I don't know, because I haven't looked at the -- at what the
17 requirement is with respect to disclosure -- but I will say
18 this, it's now interrupted the proceeding, it's made it more
19 difficult for me to understand the position of the parties,
20 and I think it abrogates your responsibility as an employee
21 and representative of the United States government and
22 particularly this agency.

23 But that's sort of the theme I see in this whole
24 investigation.

25 MR. GORJI: Your Honor, if I may address that? I

1 apologize if that is what has occurred in this case.

2 THE COURT: You know what my mother used to say?
3 My mother, bless her heart, who is now dead, used to say when
4 I apologized, she said you can't live a life of I'm
5 sorries. Now you are living through a hearing of I'm sorries
6 because this is now your third apology.

7 But it comes from the fundamental refusal of you
8 and your colleagues with candor and with transparency to say
9 here is where we are going on this.

10 Your whole position on this is that I don't have
11 jurisdiction to do this, and that has -- and that's all you
12 briefed is that I am not authorized to review the authority
13 of your agency under Section 5 to conduct this
14 investigation.

15 And so you are relying upon those what you think
16 are bright line rules about a section, which in my course of
17 doing this for for ten years is fairly ambiguous to me.
18 But this is the first time where it hasn't been a direct
19 consumer action, and I frankly think there is a legal
20 question.

21 Now, the question for me is whether or not I have
22 the authority to decide that or whether there is some other
23 process that has to first be exhausted or however you want to
24 advocate it through in order to get a final opinion that can
25 be appealed to a court.

1 MR. GORJI: Your Honor, the jurisdictional
2 arguments are the primary arguments we do make. We do also
3 make the 12 (b) (6) arguments, Your Honor, that do not deny
4 your authority but that we believe the causes of action fail
5 to state a claim.

6 But I would just like to put something in
7 perspective on behalf of the government here, Your Honor,
8 which is the history of acrimony that you perceive, this is a
9 case that I was just very recently assigned to along with
10 co-counsel here. Counsel who was on this case is no longer
11 with the Department of Justice.

12 And so I just became aware of this transcript last
13 week, Your Honor. And so there certainly wasn't any --

14 THE COURT: That's not the defendant's or my fault
15 or my problem. That's your problem. If you want to switch
16 lawyers, you switch lawyers.

17 And if you are talking about the fellow who was
18 here on the CID, I could tell you as a result of that hearing
19 that there was already a history of acrimony and I think on
20 behalf of the agency the exertion of authority in a
21 mean-spirited way.

22 MR. GORJI: Well, Your Honor, I can just say
23 that --

24 THE COURT: And you might -- you know, I'm
25 not saying that -- if you are just new to this case, which

1 I think is the reason why I put this off, to allow you time,
2 that I would hope that change in lawyers would change
3 atmosphere.

4 MR. GORJI: Your Honor, there was no intention to
5 hide anything from plaintiff here. We disclosed this in our
6 filing, and, you know, if counsel had asked me what part
7 exactly of the transcript are you hoping to make use of,
8 I certainly would have answered that question.

9 THE COURT: Well, I know, but they are not used to
10 you. They are used to the people who preceded you.

11 And it's hard for you to say this is a new day, and
12 I suspect you didn't call them and say, look, we have got to
13 change the atmosphere in this case, I understand that it
14 hasn't gone well, we understand what your complaints are --
15 and I would hope that you would understand their
16 complaints -- but we want to get on a platform that allows
17 whoever hears this in whatever forum, that would facilitate
18 the communication and entry into the record of information
19 that would allow a thoughtful, just decision on a case that
20 I think needs a thoughtful, just decision.

21 And I think especially when lawyers change, that
22 it's the responsibility of the new lawyers to reach out and
23 say we are going to handle this in the way that, one,
24 advocates on behalf of our client, but at the same time, we
25 recognize we are the government and we do want to be fair,

1 and we want to go down to Atlanta on this hearing that has
2 been put off at our request, which I did because of people's
3 personal commitments, and while my schedule is not very fluid
4 or is not fluid at all anymore and it has very little
5 capacity, it made sense to do that, and I did.

6 MR. GORJI: Well, we appreciate that.

7 THE COURT: But I expected this to go a lot better
8 than it is.

9 MR. GORJI: Again, Your Honor, there was no
10 intention to hide anything. By bringing the fact that we
11 were going to use this transcript to counsel's attention,
12 I thought that we had taken care of our obligations to alert
13 them to the fact that we potentially --

14 THE COURT: Well, I don't know, because, one,
15 nobody has told me what the obligation is, nobody told me
16 that there was going to be a dispute about this.

17 And you didn't either, Mr. Raider. You were on
18 notice. You didn't say, by the way, we are going to have a
19 problem with that, let me give you a heads-up that that's
20 going to happen. But you haven't said that.

21 In fact, I think you are kind of shooting from the
22 hip to say, well, we don't want it to come in now, not even
23 really understanding what they want to come in, even though
24 there are four of you here today.

25 I hope you are not paying them all, because if you

1 are, no wonder you are going broke.

2 MR. RAIDER: Your Honor, the basic points, really,
3 have already been made without the use of the transcript
4 that --

5 THE COURT: Well, you know, this is -- you don't
6 get to try the case for them, as much as you would like to.

7 MR. RAIDER: No, I'm not -- I understand.

8 THE COURT: The question is what -- and I don't
9 want to waste any more time. We spent half an hour on
10 this.

11 Is there some way for you to draw to my attention
12 that would not disclose in this public forum information that
13 you all agree at the time it was taken was deemed to be
14 confidential or protected, that you could get whatever --
15 there can't be that much in this transcript that relates to
16 that, that you could highlight those for me? And you can
17 even do it today, and say here is what we would show him, and
18 I would determine whether or not it is or is not consistent,
19 and we can move on?

20 MR. GORJI: Your Honor, there really is only about
21 two pages of text, and we could confer with counsel to decide
22 if they are -- to come up with a proposal for Your Honor, if
23 that's --

24 THE COURT: Why don't we do that now? Because
25 I don't want this hanging over my head any longer than it has

1 been.

2 (*Counsel confer.*)

3 MR. RAIDER: Your Honor, we have no objection to
4 the pages pointed out to us.

5 MR. GORJI: Your Honor, if I may approach the
6 witness and provide him with this transcript?

7 THE COURT: You may.

8 BY MR. GORJI:

9 Q. Showing you your transcript from the FTC administrative
10 proceeding on February 10th, 2014, it has your name on
11 it. Do you recall giving testimony in that proceeding?

12 A. Yes, I do.

13 Q. And the attorney who asked the questions was
14 Alain Sheer?

15 A. Correct.

16 Can you point out what testimony we are talking about?

17 Q. Yes, I'm going to draw your attention to page 130, line
18 25.

19 A. Can I read -- can I read this first?

20 Q. Yes.

21 A. What is the two pages? Can you tell me the beginning
22 and the end, please?

23 Q. Yes, I am going to tell you. Starting on page 130, line
24 25, through 131, which is this page, line 12. If you would
25 take a look at that?

1 A. That is the whole part of the two pages are these two
2 things? Okay, so you don't mean pages of this; you mean
3 transcript pages, okay.

4 Okay. So you are ending -- I'm sorry, you are ending on
5 131, line what?

6 Q. Line twelve.

7 A. Line twelve, okay. I'm sorry, thanks.

8 Okay, I have read it. Thank you.

9 Q. Was it your testimony there that you were asked, How
10 does Obamacare fit into the decision to wind down LabMD?

11 Answer: It's creating huge anxiety, destruction,
12 consolidation to our customer base.

13 Question: What does that mean for LabMD?

14 Answer: That means our customers are in survival mode
15 and, therefore, are having to either sell their practices or
16 merge with others and send their specimens to where they are
17 told to send them, not where they want to send them.

18 Question: Is LabMD one of the laboratories to which
19 your clients are told to send their specimens?

20 Answer: No.

21 A. Okay.

22 Q. Is it that your testimony there?

23 A. That was my testimony, yes.

24 Q. Also I'm going to draw your attention to page 60.

25 THE WITNESS: Okay. So did you look at this

1 additional? Okay.

2 BY MR. GORJI:

3 Q. I'm going to draw your attention to page 60 --

4 THE WITNESS: And my lawyers were okay with that
5 other part?

6 MR. RUBINSTEIN: Yes.

7 THE WITNESS: Okay. Thank you.

8 MR. GORJI: I believe your lawyers do not object.

9 MR. RUBINSTEIN: No objection.

10 THE WITNESS: Okay.

11 BY MR. GORJI:

12 Q. I will point you to page 60, and if you start with line
13 nine and go through line eleven?

14 A. Uh-huh.

15 Q. Was that your testimony there?

16 A. At that moment, yes.

17 Q. When you say that moment, that was on February --

18 A. -- 10th, 2014.

19 I mean, this is like out of context here, so let me just
20 see what else is going on here.

21 Other than that, I don't know at the moment. It depends
22 on -- other than that I didn't know at the moment, I didn't
23 know the future plan -- I didn't know the factors of the
24 future plan pertaining to Obamacare, and other than that,
25 I didn't know other factors. I --

1 Q. So you agreed you were asked on line nine: What's your
2 future plan for LabMD?

3 Answer: It depends on Obamacare, and other than that,
4 I don't know.

5 A. And then, I didn't know what the future plan was. But
6 I didn't say it was the only Obamacare. Okay.

7 Q. You can hold on to that.

8 A. Okay, thanks. Are we done for now? No? All
9 right. Excuse me.

10 Q. Now, you mentioned that your VP of operations left the
11 company?

12 A. Correct.

13 Q. Did he indicate whether or not Obamacare impacted his
14 decision to leave?

15 A. No.

16 Q. And you haven't provided an affidavit from your vice
17 president of operations, have you?

18 A. Well, he's no longer the vice president of operations.

19 Q. You haven't provided an affidavit from your former vice
20 president of operations; is that correct?

21 A. You deposed him.

22 Q. You also claim that you have not been able to obtain
23 insurance as a result of the FTC investigation. Did you
24 inquire to the insurance providers whether or not it was the
25 fact that there was an investigation or the fact that

1 customers' personal information was found in places that it
2 shouldn't have been that gave them pause?

3 A. Well --

4 Q. Did you ask them that question?

5 A. I wouldn't have asked that question because that's an
6 allegation about customers' information found in places other
7 than it should have been. That's not a question I would have
8 asked.

9 And whether that's true or not, when things are found in
10 other places, that does not incite a government
11 investigation. There are breaches that are hundreds of times
12 greater than mine that have gone on, if mine had a breach,
13 which we don't think it did.

14 So, no, that is not a question I would have asked. And
15 because I was -- well, first of all, they won't speak to me
16 directly. They tend to go through my broker. These
17 insurance underwriters don't want to talk directly to the
18 customer. They are going to go through the broker.
19 So this is why the broker sent me the e-mail and conveyed
20 information to me.

21 But according to the broker, it was the FTC
22 investigation and the costs they are looking at. They are
23 looking at risks and dollars.

24 Q. Certainly one of the risks that they would probably be
25 interested in is whether or not your protected information is

1 adequately protected; is that correct?

2 A. No, because it's not a cyber security policy. They are
3 interested in -- well, I would say they are interested in
4 whatever can cost them, and whenever there is -- nothing
5 scares an underwriter greater than the unknown or nothing
6 scares a medical underwriter than a chronic disease.

7 And so I'm assuming since the only response that came
8 from them -- and I didn't have direct conversations with them
9 other than talking to my broker -- was that it was the
10 unknown of the FTC investigation.

11 Q. Did you get an affirmative statement from the insurance
12 company that they would cover you if the FTC investigation
13 was enjoined?

14 A. No, I didn't.

15 Q. How many insurance companies have you contacted to
16 obtain insurance coverage?

17 A. Well, I contacted brokers. They contacted insurance
18 companies.

19 Q. Do you know how many insurance companies?

20 A. Approximately -- I think approximately a dozen,
21 approximately. I am not quite sure. At least, at least
22 seven or eight. But, you know, the brokers don't want to
23 name names.

24 Q. And you don't have an affidavit from any of your brokers
25 explaining why you have been denied coverage?

1 A. No, I don't have an affidavit from them.

2 MR. GORJI: One moment, Your Honor.

3 Nothing else, Your Honor.

4 Thank you, Mr. Daugherty.

5 THE WITNESS: Did you want this back?

6 MR. GORJI: You can keep it.

7 THE WITNESS: Okay. Thank you.

8 THE COURT: Any redirect?

9 MR. RAIDER: Just one quickly on redirect,
10 Your Honor.

11 -- -- --

12 REDIRECT EXAMINATION

13 BY MR. RAIDER:

14 Q. Your deposition was February 10, 2014. What was the
15 status of LabMD's cancer detection testing services on that
16 date?

17 A. We were doing no more. That was about three and a half
18 weeks out from our last report out.

19 MR. RAIDER: Thank you. No further questions.

20 THE COURT: All right. Thank you. You may return
21 to counsel table.

22 THE WITNESS: Thank you.

23 THE COURT: Call your next witness, please?

24 THE WITNESS: Should I leave this here?

25 MR. RAIDER: Thank you, Your Honor. We call

1 Mr. Cliff Baker. And Mr. Meyer will handle that
2 examination.

3 -- -- --

4 CLIFF BAKER

5 being first duly sworn by the Courtroom Deputy Clerk,
6 testifies and says as follows:

7 -- -- --

8 DIRECT EXAMINATION

9 BY MR. MEYER:

10 Q. Mr. Baker, could you state your full name and address
11 for the record?

12 A. Cliff Baker, 4850 Topeka Court, Dunwoody, Georgia.

13 Q. And where are you employed?

14 A. A company called Meditology Services based in Atlanta.

15 Q. In what capacity?

16 A. I'm the CEO and founder of the company.

17 Q. And what exactly is your role as the CEO?

18 A. Obviously oversee the running of the company, but I also
19 lead a practice that focuses on privacy and security in
20 healthcare, consulting with companies around privacy and
21 security in healthcare.

22 Q. And when you say consulting about privacy and security,
23 what exactly do you mean?

24 A. My career has been focused on helping primarily
25 healthcare organizations adopt security practices that first

1 and foremost align with the security rule and then generally
2 good practices to have a place to protect information.

3 Q. What were you asked to do in this case?

4 A. I was asked by counsel to review Dr. Hill's report and
5 compare it to my understanding of the HIPAA obligations for
6 companies in the healthcare industry.

7 Q. And what additional experience do you have to make such
8 an analysis?

9 A. As I mentioned, I spent almost twenty years now helping
10 organizations in the healthcare industry implement security
11 controls to comply with HIPAA.

12 Prior to starting Meditology Services, I spent about
13 fourteen years at a company called PriceWaterhouseCoopers
14 primarily in the healthcare -- leading their healthcare
15 security practice and consulting with their clients around
16 implementing security practices.

17 After I left PriceWaterhouseCoopers in 2008, I was the
18 chief strategy officer and architect for a framework called
19 the High Trust Security Alliance, which essentially was a
20 number of organizations across the healthcare industry that
21 came together to try and define a reasonable and appropriate
22 standard for the industry so the industry could proactively
23 implement controls for the healthcare industry.

24 Q. And based on that experience, could you briefly state
25 any opinions you reached regarding the standards articulated

1 in Dr. Hill's report?

2 A. The most troubling aspect of the report is that Dr. Hill
3 doesn't take into consideration any aspects of scalability in
4 terms of what's reasonable and appropriate for an
5 organization of the size of LabMD to implement security to
6 comply with HIPAA security requirements, which has really
7 been the primary driver for security requirements for the
8 industry.

9 And so when I read Dr. Hill's report, it is out of line
10 with the expectations of organizations of the size of LabMD.

11 Q. Is it your understanding that LabMD is a HIPAA-covered
12 entity?

13 A. It is my understanding that they are a HIPAA-covered
14 entity.

15 Q. And based on your experience, do you have any reason to
16 believe that the standard articulated by Dr. Hill would
17 create confusion amongst HIPAA-covered companies?

18 A. Absolutely. The industry continuously is looking for
19 clarification and specificity from the regulators to make
20 sure that they understand what their obligations are, and
21 when a regulating body makes a judgment based on some
22 standard, the industry reacts and the industry tries to
23 understand what their obligations will be as a result of that
24 ruling.

25 So I think the position that Dr. Hill takes is

1 contradictory to the ten years of experience we have had with
2 HHS and understanding their expectation of the industry.

3 Q. And following up on that, I want to go through some
4 particular topics. What is scalability?

5 A. In the creation of the HIPAA rule, a key tenet of the
6 HIPAA rule was to implement controls that were reasonable and
7 practical for the resources, capacity, skills of an
8 organization.

9 HIPAA recognizes that the healthcare industry ranges
10 from large multinational companies to one-physician practices
11 with no IT resources -- probably no IT resources on staff,
12 maybe an office manager at best. And so HIPAA had to be able
13 to specify requirements that would be adopted for the largest
14 companies and the smallest companies.

15 Obviously specifying specific requirements for each of
16 those extremes is difficult, and so HIPAA created this
17 concept of a risk assessment which allowed organizations to
18 analyze their exposures and to make decisions that related to
19 the security controls that were appropriate and that they
20 could really have the resource, capacity and skills to
21 implement.

22 Q. And how does Dr. Hill address scalability?

23 A. Her primary considerations for scalability is the number
24 of records that LabMD holds. And, candidly, the number of
25 records at LabMD is minute compared to larger organizations

1 that offer similar services.

2 And then she doesn't really ever consider the type of
3 organization they are in the industry, the number of
4 employees that they have, the number of resources that they
5 have hired from an IT and security perspective. None of
6 those considerations come into her -- the basis of her
7 opinion in her report.

8 Q. How significant is the difference between the standard
9 Dr. Hill articulates and what HIPAA requires?

10 A. From my perspective, it's significant. Imposing
11 requirements on an industry that are not practical and
12 reasonable, you know, really have a contrary impact to what I
13 believe the regulators are trying to do, which is to make
14 sure that appropriate security controls are in place.

15 And so imposing requirements that don't address this
16 kind of scalability aspect will distract the industry in
17 large part because now they have to interpret and figure out
18 how they are going to implement requirements that are
19 misaligned with expectations that have been set for them for
20 the past ten years.

21 Q. How important is scalability for a company the size of
22 LabMD?

23 A. It's extremely important. Textbook security
24 requirements or controls, if you read textbook requirements
25 and you put the same requirements in front of a large

1 multinational company, you know, they have more security
2 resources than LabMD has employees. And so the skills and
3 investments that they will make around security would
4 probably exceed the total revenue that LabMD probably pulled
5 in its entire existence.

6 So it's incredibly important, because if the regulators
7 want real controls to be implemented, they have to make them
8 practical and they have to make them reasonable and they have
9 to impose expectations that small organizations can actually
10 achieve.

11 Q. What is integrity monitoring?

12 A. Dr. Hill refers to this concept called file integrity
13 monitoring, and it is essentially technology used to monitor
14 any change to files on an issue.

15 So it essentially looks for any change, whether you save
16 a file or you implement a new file or put a new file on a
17 computer, it will send off an alert to somebody. And
18 somebody will have to read that alert, investigate it and
19 respond to it.

20 Q. Does HIPAA require file integrity monitoring?

21 A. It doesn't specifically require file integrity
22 monitoring at all.

23 Q. And what does Dr. Hill say in her report?

24 A. This is one of the key controls that she says LabMD
25 should have had in place. And I think it's a classic example

1 of where her report is out of alignment with the expectations
2 that HHS sets for the industry.

3 As an example, Dr. Hill often in her report refers to
4 free software or inexpensive software that can be implemented
5 to achieve some of these controls. What she doesn't consider
6 is the resource requirements to follow up, investigate,
7 configure, implement those tools.

8 And file integrity monitoring particularly has a
9 significant resource impact on an organization because it's
10 constantly sending out alerts that need to be investigated.

11 Furthermore, Dr. Hill recommends that file integrity
12 monitoring be implemented on a workstation. So on occasion
13 for large organizations you will see it on servers.

14 The reason I'm making that distinction is when a user is
15 on a workstation, they are often changing files. You are
16 opening Word documents, you are opening Excel documents, you
17 are opening and closing files.

18 With that kind of software, there is a potential for an
19 alert to be sent out every time a file is changed, and you
20 can imagine the resource impact that that's going to have on
21 the resources of a particularly small organization.

22 Q. For a company the size of LabMD, what would you
23 recommend with respect to file integrity monitoring in order
24 to be in compliance with HIPAA?

25 A. HIPAA is based on a risk assessment first.

1 Fundamentally HIPAA requires risk assessment. And so
2 we'd work with a company the size of LabMD, understand their
3 exposures, and essentially put a measured program in place to
4 implement security over time.

5 We would start with some limited monitoring that would
6 be in place probably on the servers versus their workstations
7 and then evolve that over time.

8 The primary reason we would not start with file
9 integrity monitoring is we know that it would overwhelm their
10 resources and that the net impact would be that security
11 would not be implemented, information would not be well
12 protected because the resources would not have enough
13 capacity to actually focus on the things that matter.

14 Q. All right. What is encryption?

15 A. Encryption is a process of turning readable information
16 into unreadable information that is only accessible or
17 unlocked for the individuals that have keys to unlock that
18 information, in laymen's terms.

19 Q. Does HIPAA address encryption?

20 A. It does address encryption.

21 Q. How?

22 A. It's an addressable requirement.

23 And there is a distinction, an important distinction in
24 the rule. There are required items and addressable items in
25 the rule.

1 And HHS guidance for addressable items is that the
2 decision around how to achieve those requirements,
3 addressable requirements, should be based on the risk
4 assessment, and then HHS essentially provides options.

5 If the organization does a risk assessment and believes
6 that there is an exposure, believes that they have ways that
7 cost and impact from a resource capacity on the organization
8 in terms of implementing that control to mitigate the
9 exposure, they should go ahead and do it.

10 On the other hand, in evaluating the exposure against
11 the cost and resource capacity to achieve that control, if
12 that cost and resource capacity exceeds the capabilities,
13 they can explore alternate options.

14 If no alternate options exist, then they don't have to
15 implement that control.

16 Q. What is Dr. Hill's opinion with respect to encryption?

17 A. Dr. Hill's opinion is pretty black and white, that
18 encryption should be implemented.

19 Most troubling I think about her report is that she
20 makes reference to encryption and risk. What I mean by that
21 encryption stored in databases on servers.

22 And candidly, you know, across all industries, that is
23 not generally an adopted practice, primarily because it has
24 an impact on the processing speed and performance of
25 systems. We are starting to see more and more of that kind

1 of control implemented, but mostly for large organizations
2 that have the resource capacity to implement those kind of
3 controls.

4 It's very unusual -- I have never seen an organization
5 the size of LabMD implement encryption and risk.

6 Q. What would you recommend to an organization the size of
7 LabMD with respect to encryption in order to comply with
8 HIPAA?

9 A. Again, it would be based on the risk assessment, and
10 I would recommend implementing controls where I know they can
11 achieve the objectives required for encryption.

12 So for example, for any access to their website, if
13 there was particular health information exchanged, I would
14 expect that information is encrypted.

15 Q. You mentioned the risk assessment throughout your
16 testimony now. Does Dr. Hill have an opinion regarding risk
17 assessment?

18 A. She certainly does.

19 Q. And what is it?

20 A. You know, interestingly, we both refer to the same
21 standard reference for risk assessment, which is the NIST
22 Security Series Reference 800-30, which is a
23 government-published approach for performing a risk
24 assessment.

25 Where Dr. Hill and I have a departure in kind of

1 methodology, she immediately will go in her report to
2 suggesting that the organization implement technical tools to
3 achieve the risk assessment.

4 And again I think this is based on her experience in
5 kind of, you know, she seems to have a very technically kind
6 of focused career, technology focused career, and so her
7 immediate response in terms of this risk assessment is to
8 implement a number of technology solutions.

9 As I mentioned to you before, the license cost for those
10 solutions may not be high. The resource cost to actually
11 manage and implement those solutions is significant.

12 And when you look at the way HIPAA and HHS guides the
13 industry in terms of doing a risk assessment, it's certainly
14 not starting with implementing tools. It's with a process
15 and a mind-set and a methodology, candidly mostly relying on
16 manual methods to assess risk.

17 I think that kind of highlights the fundamental
18 distinction between Dr. Hill's report and generally where HHS
19 is guiding the industry.

20 Q. In offering those opinions, does Dr. Hill rely on any
21 published materials from FTC?

22 A. She doesn't, which I found interesting.

23 I would have thought that the expert -- the expert
24 witness for the FTC would have been referencing FTC guidance
25 for security requirements. She did not reference that in her

1 report, that I recall.

2 Q. Are you aware of the FTC publishing data security
3 standards for medical service providers other than what's in
4 Dr. Hill's report?

5 A. I am not aware. In my line of business, I don't rely on
6 FTC guidance for security requirements for my client base.

7 Q. And you have been in that line of business for almost
8 twenty years; right?

9 A. That's correct.

10 Q. And in that time, are you aware of any statements made
11 by the FTC expressing their authority to impose requirements
12 on protected health information in excess of HIPAA?

13 A. I am not aware of those requirements.

14 MR. MEYER: No further questions, Your Honor.

15 THE COURT: I want some clarification to make sure,
16 see if my understanding about this is correct. That -- and
17 I guess this is an allegation.

18 The allegation is that the security breach here was
19 the disclosure of certain patient records. And I don't know
20 the quantity of the patient records that are alleged to have
21 been disclosed, but apparently it was some patient
22 information; is that right?

23 MR. RUBINSTEIN: Your Honor, Reed Rubinstein. If
24 I might?

25 It's not clear. We have heard different things in

1 the course of the administrative hearing. Originally there
2 was a focus --

3 THE COURT: Well, what's your understanding about
4 what went from LabMD outside of the company to others, or are
5 you claiming that nothing did?

6 MR. RUBINSTEIN: There are allegations that --

7 THE COURT: No, what's your understanding? Have
8 you reached a conclusion that certain patient information was
9 disclosed outside the company?

10 MR. RUBINSTEIN: Our understanding, based on the
11 testimony that's been taken to date --

12 THE COURT: Well, you are the lawyers for the
13 company.

14 MR. RUBINSTEIN: That's correct, but --

15 THE COURT: Have you reached any conclusion that
16 information that was private for patients that was delivered
17 to you by these people that were hiring LabMD got disclosed
18 outside the company?

19 MR. RUBINSTEIN: We do not believe that
20 information -- patient PHI has been disclosed outside the
21 company based on what we have learned on discovery.

22 And the reason for that, among other things,
23 testimony of the FTC's experts with respect to the expected
24 rate of identity theft. In this case, there is no single
25 plaintiff, no single person who has alleged --

1 THE COURT: All right. My question was do you
2 know. You are saying there is not.

3 Second, did somebody load a file-sharing program on
4 any LabMD computer?

5 MR. RUBINSTEIN: Yes.

6 THE COURT: And did you do any investigation to see
7 whether or not any information was accessed through the use
8 of that file-sharing program from somebody outside the
9 company?

10 MR. RUBINSTEIN: I believe in approximately 2008,
11 LabMD was informed that file-sharing software was on the
12 computer. LimeWire, which is used primarily for audio
13 files.

14 There was an investigation done by the company.
15 This was contrary to the company's policies, and it was
16 removed.

17 The FTC investigation began two years --
18 approximately two years thereafter, and there are allegations
19 with respect to two specific alleged data breaches.

20 The first related to an insurance agent file, a
21 1718 file. A second related to certain day sheets, which
22 were actually printed forms. They had nothing to do with
23 data security in the sense that we are using it.

24 It is not clear to us still today and there is no
25 evidence in the record that demonstrates how exactly the 1718

1 file, if it did, got out. That's one of the things that's
2 still, frankly, developing.

3 But as I said, to our knowledge and as far as we
4 can tell to the government's knowledge, there is not a single
5 case of identity theft attributable to the alleged data
6 breach.

7 THE COURT: Well, what is it that the FTC claims
8 was the data security breach?

9 MR. GORJI: Your Honor, there are two instances,
10 one being that the Sacramento, California, Police Department
11 found information belonging to LabMD's customers in the hands
12 of identity thieves.

13 Now, that was reported to LabMD. My understanding
14 is LabMD actually informed customers that there had been
15 a --

16 THE COURT: And when was that?

17 MR. GORJI: That was October 2012. I don't know
18 when LabMD actually informed their customers or there was a
19 disclosure.

20 THE COURT: And how did the police department know
21 that it originated from LabMD, and in what form did they have
22 it?

23 MR. GORJI: Your Honor, there was documentation
24 that indicated it pertained to LabMD, I believe.

25 THE COURT: You mean papers?

1 MR. GORJI: Documents, papers.

2 THE COURT: All right. So -- and where did the
3 police department claim that the papers -- how were the
4 papers obtained?

5 By papers, you mean paper documents, that somehow
6 they got hold of some paper documents with some patient
7 information on it? Is that what the allegation is?

8 MR. GORJI: Yes, Your Honor. My understanding is
9 they were in possession of the individuals who pled no
10 contest to the state charges of identity theft.

11 THE COURT: Well, if they pled no contest, they
12 probably cooperated. Did they tell you where they got the
13 papers?

14 MR. GORJI: Your Honor, if I might inquire?

15 Your Honor, I don't have information as to how the
16 documents and the information was obtained by the identity
17 thieves.

18 THE COURT: Well, has anybody from the FTC gone out
19 and interviewed the people who pled *nolo* to that to find out
20 where it came from, to see whether or not there was indeed a
21 security breach?

22 Let me tell you something, these are the most
23 simple questions of this investigation. That you are
24 claiming that some police department prosecuted some people
25 for having possession of information which you are now

1 claiming wrongfully was not protected by LabMD, and you can't
2 even tell me whether or not you have interviewed the people
3 who had the data to find out where they got it to see whether
4 or not there was a security breach or not? And yet you have
5 implemented and instituted this investigation?

6 And this is your case. You are new -- I know you
7 might be new on it, but for heaven's sakes, you are arguing
8 to me that there is a hearing on May 20th and you don't even
9 know.

10 MS. FASCETT: Your Honor, if I may just explain,
11 just for clarity, not as an excuse. The FTC attorneys that
12 are handling the administrative proceeding in that hearing,
13 they I'm assuming definitely know these details. They are
14 not present. They are not here today.

15 We are just -- we were just brought in from DOJ to
16 represent this complaint in this action. So that's part of
17 why we don't have these facts. But we represent the FTC here
18 and we can get these facts for you.

19 MR. RUBINSTEIN: Your Honor, if I could?

20 THE COURT: I'm not --

21 MR. RUBINSTEIN: I --

22 THE COURT: Sit down.

23 MR. GORJI: Your Honor, my --

24 THE COURT: So where are those lawyers? Are they
25 too busy to come to Atlanta today?

1 MS. FASCETT: Well --

2 THE COURT: Is that one of them sitting back there
3 in the gallery?

4 MS. FASCETT: No, she's a U.S. Attorney here in
5 Atlanta, unrelated.

6 THE COURT: How about this other fellow back there,
7 is he an FTC lawyer too?

8 MR. MARCUS: Your Honor, we have a gentleman here
9 from the FTC.

10 THE COURT: Are you involved in this
11 investigation?

12 MR. MARCUS: I am personally not involved in the
13 investigation.

14 THE COURT: Okay. So you are off the hook.

15 So far I have got four lawyers here and none of
16 them are involved in the investigation. How about --

17 MR. MARCUS: We do have are a lawyer who is
18 involved in the investigation.

19 THE COURT: And what's your name?

20 MR. SCHOSHINSKI: Good morning, Your Honor.
21 Robert Schoshinski. I'm assistant director in the Division
22 of Privacy and Identity Protection.

23 THE COURT: All right. So in this case, what
24 investigation has been made as to the source of the documents
25 that the police department out in California found?

1 MR. SCHOSHINSKI: Your Honor, the complaint
2 counsel, so that is the FTC counsel who is litigating the
3 complaint in the administrative action, noticed the
4 depositions of the two individuals who pled no contest to
5 identity theft.

6 One they could not serve because she was just
7 simply not findable. The other one was in jail. We --

8 THE COURT: Did you try to find her?

9 MR. SCHOSHINSKI: Yes, we did, Your Honor. We
10 hired several process servers. They made many attempts to
11 try to find her but were unable to serve her.

12 THE COURT: And when did you first try to serve
13 her?

14 MR. SCHOSHINSKI: Your Honor, I don't have the
15 exact dates, but --

16 THE COURT: Well, give me an approximation.

17 MR. SCHOSHINSKI: Your Honor, I would say late
18 2013, early 2014.

19 THE COURT: So really late in the game, you finally
20 decided that it made sense to go and find out with respect to
21 one of the allegations that's the basis of your investigation
22 that's been ongoing for months, because the CID was something
23 I dealt with some months ago, that you finally decided -- or
24 not you, but your lawyers finally decided that maybe it would
25 be good to try to find the people who actually had the

1 information to determine where they got it?

2 MR. SCHOSHINSKI: Yes, Your Honor.

3 THE COURT: Does that strike you as odd?

4 MR. SCHOSHINSKI: Your Honor, it doesn't strike me
5 as odd. It's what --

6 THE COURT: Does it strike you as late?

7 MR. SCHOSHINSKI: Your Honor, it strikes me as the
8 normal course of the investigation.

9 THE COURT: Boy, that's a sad comment on your
10 agency, that you would wait until months before a hearing and
11 months after you instituted an investigation on a principal
12 claim that you are asserting, that you have not even taken
13 any effort to interview the people that you claim had the
14 documents that underlie the charge of a security
15 breach. That strikes me as almost being unconscionable.

16 And how much money -- how much activity was there
17 before you served those subpoenas trying to get the
18 information from LabMD with respect to a security breach that
19 you don't even know how it occurred? How much activity?

20 MR. SCHOSHINSKI: Your Honor, how would you like me
21 to estimate?

22 THE COURT: Let's start in months.

23 MR. SCHOSHINSKI: Well, Your Honor, I believe the
24 investigation began in January of 2010.

25 THE COURT: Okay. So three years before you tried

1 to subpoena them?

2 MR. SCHOSHINSKI: Your Honor --

3 THE COURT: I'm sorry, two and a half years.

4 MR. SCHOSHINSKI: Your Honor, the knowledge of this
5 incident didn't occur until after the CID enforcement hearing
6 up here in Atlanta. That's when we were notified that this
7 incident had occurred, in October of 2012.

8 THE COURT: So you found out about the -- the
9 incident you are talking about is the California police
10 incident?

11 MR. SCHOSHINSKI: That's correct, Your Honor.

12 THE COURT: All right. And how soon after you
13 found out about the incident did you try to contact the
14 police authorities in California to find out what they knew
15 about the source of the information?

16 MR. SCHOSHINSKI: Immediately.

17 THE COURT: And what did they tell you?

18 MR. SCHOSHINSKI: They told us that they did not
19 know.

20 THE COURT: And then what did you do next, and how
21 soon did you do it?

22 MR. SCHOSHINSKI: We shared the information with
23 LabMD concerning the -- what we found out once we were able
24 to confirm that it was LabMD's information, and we then
25 attempted to find out further from the California police

1 department what they knew about the source of this
2 information.

3 THE COURT: And what did they tell you they knew
4 about the source?

5 MR. SCHOSHINSKI: They told us they were not able
6 to get the source from the defendants in the case.

7 THE COURT: Did you talk to the prosecutor of the
8 case as well?

9 MR. SCHOSHINSKI: I don't believe so, Your Honor.

10 THE COURT: And so you tried to track down one of
11 the two defendants. Did you try to track down the second of
12 the two defendants?

13 MR. SCHOSHINSKI: Yes, Your Honor. We actually
14 obtained service on the second defendant, who was in
15 jail. We noticed his deposition in the action, went to take
16 his deposition, and he pleaded the Fifth Amendment and
17 refused to answer questions.

18 THE COURT: So sitting here today, you have no idea
19 where the documents came from, whether they came from LabMD
20 or some other source? Is that a fair thing to say?

21 MR. SCHOSHINSKI: No. We believe they were LabMD's
22 documents.

23 THE COURT: Well, they might have been LabMD's
24 documents, but you don't know how they got into the
25 possession of the two individuals that you tried to contact

1 that pled guilty to this offense?

2 MR. SCHOSHINSKI: That's correct, Your Honor.

3 THE COURT: So you have no information to establish
4 how those documents were obtained; is that right?

5 MR. SCHOSHINSKI: That's correct, Your Honor.

6 THE COURT: And you are still proceeding on this
7 claim?

8 MR. SCHOSHINSKI: Yes, Your Honor, because the
9 claim is not concerning that incident alone. It's
10 concerning --

11 THE COURT: All right. But are you still
12 proceeding on that claim?

13 MR. SCHOSHINSKI: We are proceeding on that
14 evidence, Your Honor.

15 THE COURT: And that evidence relates to other
16 claims, because you have other documents that were found in
17 other places?

18 MR. SCHOSHINSKI: That evidence relates to the
19 potential injury suffered by consumers as a result of
20 exposure of this information.

21 THE COURT: Are you serious about that last
22 response?

23 MR. SCHOSHINSKI: Yes, Your Honor, I am.

24 THE COURT: So you don't know where the documents
25 came from, you don't know how these people got the possession

1 of it, you don't know whether they originated from LabMD or
2 some other place, but you are going to use that to show that,
3 because they committed identity theft, that certain
4 individuals were damaged by documents, the source of which
5 you don't even know?

6 MR. SCHOSHINSKI: Yes, Your Honor.

7 THE COURT: Holy cow.

8 So what's the other incident that you are relying
9 on?

10 MR. SCHOSHINSKI: The other incident is the
11 exposure of the insurance agent file of several thousand
12 consumers.

13 THE COURT: And when was that?

14 MR. SCHOSHINSKI: That was in 2008, Your Honor.

15 THE COURT: And that was through the file-sharing
16 program?

17 MR. SCHOSHINSKI: That's correct, Your Honor.

18 THE COURT: And how do you know that they came
19 through the file-sharing program?

20 MR. SCHOSHINSKI: We know because third parties
21 found the file on file-sharing programs.

22 THE COURT: Well, I accept that. How do you know
23 that they came through the file-sharing program that was
24 loaded on a computer at LabMD?

25 MR. SCHOSHINSKI: Based on the evidence we obtained

1 about the file-sharing program, evidence provided by LabMD
2 that showed that certain files, including this file, were
3 shared on the file-sharing program, we believe that it was
4 exposed through the file-sharing program.

5 THE COURT: And how many records were shared?

6 MR. SCHOSHINSKI: Your Honor, I don't have the
7 exact number. I believe it was nine thousand, but I'm not
8 entirely sure.

9 THE COURT: So are you aware that nine thousand
10 files ended up in some somebody else's hands that were
11 LabMD's files?

12 MR. RUBINSTEIN: Your Honor, it would be nine
13 thousand individuals. It was one file.

14 THE COURT: Well --

15 MR. RUBINSTEIN: And we --

16 THE COURT: So are you going to dance on the head
17 of a pin now too?

18 MR. RUBINSTEIN: I'm not dancing on the head of a
19 pin, Your Honor. I appeared before the administrative law
20 judge and --

21 THE COURT: You can sit down until I'm ready for
22 you.

23 MR. SCHOSHINSKI: Thank you, Your Honor.

24 MR. RUBINSTEIN: -- I told him because the FTC said
25 that the files had been shared, our position was then and it

1 remains to date that the file was taken by this third party,
2 Tiversa.

3 As you may recall, there was quite a controversy
4 with respect to the government's ability to rely on that
5 file.

6 THE COURT: It was taken by use of an
7 improperly-loaded file-sharing program.

8 MR. RUBINSTEIN: It was taken by use of a patented
9 program that Tiversa uses as part of their business model to
10 go from company to company taking files and then coming to
11 the company and saying: Nice business you have here. It
12 would be a shame if anything happened to it. Why don't you
13 hire us to remediate?

14 In fact, that's what happened here. And part of
15 this was put before --

16 THE COURT: Was that enabled by the file-sharing
17 program that was loaded by an employee on the computers at
18 LabMD?

19 MR. RUBINSTEIN: For them to be able to gain
20 access, I don't know.

21 THE COURT: Why don't you know that?

22 MR. RUBINSTEIN: Because we don't fully understand
23 the nature and extent of Tiversa's technology.

24 We attempted to ask them in deposition, and we were
25 met with objections because this is a protected confidential

1 and highly proprietary piece of software. So we still don't
2 understand to this day.

3 THE COURT: Well, you can get a protective order in
4 order to access that. Have you asked for that?

5 MR. RUBINSTEIN: I don't recall. It would be easy
6 enough to check. I can get that for you. I just don't
7 recall whether we did that in the administrative hearing or
8 not. I am certain the question was asked, and I'm certain
9 objections were interposed.

10 And we had asked -- we actually -- it is very
11 possible that we did, because we filed a motion asking for
12 discovery into the circumstances under which there was a
13 sharing of this information between Tiversa and the FTC.

14 We discovered that the FTC had worked with
15 Tiversa. In fact, Tiversa gave LabMD's file to another third
16 party.

17 THE COURT: Well, look, I'm not trying this case,
18 although I am getting a lot of information about the
19 respective positions which also is troubling on both sides.

20 But I will say --

21 MR. RUBINSTEIN: The --

22 THE COURT: So their position, which I guess they
23 are going to present somebody under oath to say that they
24 have traced information through a file-sharing program that
25 allowed some outside source, whether it's Triversa or

1 somebody else, to wrongfully access information that was on
2 LabMD's computers?

3 MR. RUBINSTEIN: I don't believe they have done any
4 independent investigation to verify what type of --

5 THE COURT: I'm not saying that. I'm saying they
6 have got an obligation to present somebody under oath to
7 testify with respect to that, and that's what the deputy
8 director's position -- you are a deputy director; is that
9 right?

10 MR. SCHOSHINSKI: Your Honor, assistant director.

11 THE COURT: All right. I would love to promote you
12 if I could, but I can't, so you are still an assistant
13 director.

14 MR. SCHOSHINSKI: It's the lowest form.

15 THE COURT: I understand. I know titles are big in
16 agencies. I have been there and played that game for a
17 while.

18 But the assistant director has just said that there
19 will be evidence presented before a judicial officer, I guess
20 an administrative law judge, in which somebody will state
21 these nine thousand individuals -- information about
22 individuals in a single record was accessed by an outside
23 source through a file-sharing program that had been installed
24 on WebMD's computers.

25 You are going to say that there is no evidence of

1 that --

2 MR. RUBINSTEIN: That's correct.

3 THE COURT: -- that that ever happened, and you are
4 going to believe that you are right, and the FTC, although
5 sometimes I wonder if they are -- just how compelling their
6 evidence is, that they are going to claim that they are
7 right, and somebody will make a determination of whether
8 there has been a breach or not.

9 Then the question is -- and I do find this -- and
10 I think I know enough about this, and I learned a lot from
11 the CID hearing -- is that the FTC is going to go into the
12 business of monitoring and investigating and regulating
13 security breaches and that they have decided I think to do
14 that within what they believe is their administrative
15 authority, because I think they went to Congress and Congress
16 wouldn't authorize that for whatever reason, whether it's
17 politics or not.

18 But I think there has been no amendment to Section
19 5 to specifically allow that. But they are taking the
20 position that they have the authority to do that.

21 MR. RUBINSTEIN: That is correct.

22 THE COURT: I think that there is a significant
23 question about whether Section 5 allows that, but I'm not
24 sure I can decide that based upon my jurisdictional
25 limitations, perhaps.

1 But I think that's what's going on here is the FTC
2 has staked out a position of regulatory authority and that
3 they are going to advocate that and they are going to advance
4 it to the greatest extent that they can.

5 You are somebody who is the -- is somebody who has
6 fallen within that ambit of claimed authority, and you claim
7 that you didn't do it. They are going to claim that you did
8 do it.

9 So there is going to be a factual question of
10 whether or not you did or did not, and then there is going to
11 be a legal question of whether or not they have the authority
12 to do what they have done.

13 MR. RUBINSTEIN: That's correct. And we are not
14 asking you to decide factual questions today.

15 THE COURT: I know, but you are asking me to take
16 jurisdiction of this, and I'm not sure I can.

17 MR. RUBINSTEIN: Well, and I'm happy to do argument
18 with respect to that.

19 THE COURT: Look, I have spent more time looking at
20 cases than you have on this, so I don't need any more
21 argument on the jurisdictional issue.

22 MR. RUBINSTEIN: Fair enough.

23 THE COURT: I mean, I do think it's strange that a
24 judge in New Jersey gets to decide the jurisdictional issue
25 because the posture of the FTC was different in that case

1 than it is in this case, and then they are arguing that,
2 although I'm co-equal to the judge in New Jersey, that
3 because it came to me a different way, that I can't.

4 I suspect that they would love to travel forward on
5 the New Jersey decision because it favors them and that they
6 will try to deny the opportunity for another judge to weigh
7 in.

8 But I think it's a significant -- you ought to find
9 a way, unless you are so hell bent on expanding this
10 jurisdiction or advocating this jurisdiction, to find some
11 way to decide this legal issue.

12 And I understand why you are doing what you are
13 doing. I have been alive long enough to understand how
14 government and their agencies work. I have been a member of
15 an agency and I understand its impact on defendants or in
16 this case on parties that are under investigation. I
17 understand that too because I have done that as well.

18 But I think that there is a fundamental
19 jurisdictional legal issue, and there ought to be some way of
20 getting a more definitive ruling than what you have right
21 now.

22 Because I would hope that you would think that in
23 this current healthcare environment, that the more
24 competition and providers there are for medical detection
25 devices or processes like those offered by LabMD, that the

1 better off the consuming public is and the better off
2 patients will be. But by your conduct, you have taken one
3 out of the market it looks like.

4 And if I was an agency head, I would say there has
5 got to be some way of being satisfied that this doesn't
6 happen again, however it happened, and to make sure that we
7 have as many providers as possible out there determining
8 whether or not people do or do not have cancer.

9 And that that would mean a good faith, transparent,
10 authentic discussion about what your concerns are, and trying
11 to get those allayed by some process which would not be a
12 twenty-year monitoring.

13 You know, I have defended people that had
14 twenty-year monitoring responsibilities by an agency, big
15 companies, and it's very, very expensive, and it's really
16 intrusive, and in my personal opinion, having been on both
17 sides, they generally are not necessary.

18 But there is never a middle ground. There should
19 be.

20 But I would think that it would be in the benefit
21 of all the parties here to say whatever happened, it can't
22 happen again, but whatever you are doing ought to continue to
23 be done, because it benefits the consuming public, which I
24 think is who you are supposed to be protecting under
25 reasonable certainties, that the consuming public would be

1 treated fairly.

2 And it's interesting the two people that didn't
3 treat the consuming people fairly are two people in jail that
4 won't even cooperate with you and one of whom you can't even
5 find.

6 But I don't think that even the FTC thinks that
7 they intentionally wanted this information to get out,
8 because they are subject to HIPAA regulations.

9 And I will say I have gone into enough doctors'
10 offices and nobody has ever had me sign a statement saying
11 that whatever the obligations are, the rights that I have
12 under the FTC are rights that I have to acknowledge and in
13 some cases give up. It's always HIPAA.

14 And I think that's what happens when you try to
15 extend into an area where you might be allowed or be
16 permitted to extend, but that assumes, especially on behalf
17 of the government, that they act reasonably.

18 And here we are, having spent now about an hour and
19 a half, not getting to the fundamental issue here, which I
20 think is how can your interest be accommodated.

21 And, Mr. Gorji, if you submitted to them a consent
22 order -- and I'm not going to consider that; I don't think
23 it's important -- but it does tell me something about your
24 agency if you say we want twenty years' worth of monitoring
25 and even suggested that was reasonable concerning this

1 company. No wonder you can't get this resolved, because if
2 that's the opening salvo, even I would be outraged, or at
3 least I wouldn't be very receptive to it if that's the
4 opening bid.

5 I don't think you believe that this is a company
6 that willy-nilly allows information to be disclosed. I also
7 believe that you don't think, if you remove yourself from the
8 nits and gnats of this dispute, that you would say it was a
9 good idea to make this provider unavailable to patients.

10 There aren't that many people doing this work as it
11 is. I have another case involving cancer detection
12 processes, and so I know just a little bit about the
13 industry, and one of the regrets of the industry is that
14 there are so few people providing these services. And
15 I think in the current healthcare environment, there will be
16 fewer.

17 It doesn't serve any of us very well. Some day you
18 are going to need one of those services. I hope it's
19 available.

20 You have been completely unreasonable about
21 this. And even today you are not willing to accept any
22 responsibility that whatever needs to be done, even if you
23 can't confirm it, that your position is going to be a
24 litigating position, and you will drag four lawyers to a
25 hearing like this.

1 I mean, I was in a big firm, but on a hearing like
2 this, we wouldn't have four lawyers here. So I don't know
3 what you are trying to accomplish, but I will tell you this,
4 you haven't.

5 And I have a firm belief that it takes two
6 unreasonable people to create an unreasonable atmosphere that
7 prohibits a reasonable result, and that's where we are.

8 Your interest is protecting the American public.
9 That's your responsibility.

10 Your interest is to help a client who I think is
11 providing a good service survive.

12 And I am confident -- I haven't been in all these
13 depositions. I know this, it's always hard to deal with
14 somebody who is changing lawyers all the time. But to the
15 extent that any of that has irritated you, Mr. Daugherty, you
16 need to settle down. I know you are upset down this, but you
17 are poisoning the atmosphere personally.

18 And if I was a lawyer representing you, the first
19 thing I would say is you have got to stop the public
20 stuff. If you want to get this resolved and do something
21 well, no government agency is ever going to treat somebody
22 who's advocating publicly and criticizing publicly. They are
23 going to be less accommodating to them. And I have told that
24 to clients over and over and over when I was a lawyer. Now
25 I get to see it from the other end, and now I'm convinced

1 that's the case.

2 So to the extent that you have gotten some
3 therapeutic value out of all this, it ought to stop, because
4 your criticism hasn't gotten you to where you want to be, has
5 it? It's gotten you where you don't want to be.

6 So I understand the legal issues. I thought as
7 I enter my sixties, one of the values I can do is give you
8 some perspective.

9 Are you a Fiske Scholar? Did you go to the
10 University of Michigan? Did one of you go to Michigan and
11 are a Fiske Scholar?

12 MR. RUBINSTEIN: I did, Your Honor.

13 THE COURT: Yeah. Are you a Fiske Scholar?

14 MR. RUBINSTEIN: Not a Fiske Scholar. I was an
15 Angell Scholar.

16 THE COURT: All right. Well, never mind. Although
17 I will tell you that the story that if one of you had been
18 that I have is working with Bob Fiske, who I think is one of
19 the finest lawyers in America, that we were once granted
20 jurisdiction, and we always, whenever somebody brought a
21 claim to us to try to request us to expand our jurisdiction,
22 we would have a roundtable discussion to say where within the
23 grant of authority to us is our jurisdiction specifically,
24 and, if not, it needs to go back to the people who are
25 entitled to grant jurisdiction, which we believe was

1 Congress, and we turn things down.

2 I think good lawyers -- and he was an agency lawyer
3 for a long time and ran the Southern District for a long time
4 as United States Attorney -- that that lesson has always
5 stuck with me.

6 So where we are now is I have given you my insights
7 about this. I understand there is no more evidence to be
8 presented.

9 I don't need any more -- I guess you can
10 cross-examine him if you want. All I hear him saying is that
11 he doesn't like your expert's report and he would have done
12 something differently and he's claimed that HIPAA is what
13 should be, because there are specific standards there --
14 I think that you will admit that there are no security
15 standards from the FTC. You kind of take them as they come
16 and decide whether somebody's practices were or were not
17 within what's permissible from your eyes.

18 I too find how does any company in the
19 United States operate when they are trying to focus on what
20 HIPAA requires and to have some other agency parachute in and
21 say, well, I know that's what they require, but we require
22 something different, and some company says, well, tell me
23 exactly what we are supposed to do, and you say, well, all we
24 can say is you are not supposed to do what you did.

25 And if you want to conform and protect people, you

1 ought to give them some guidance as to what you do and do not
2 expect, what is or is not required. You are a regulatory
3 agency. I suspect you can do that.

4 But I think that's what happens when you jump too
5 quickly into something that you want to do, and whether
6 that's circumstances or whether that's agency motivation, I
7 don't know. But it seems to me that it's hard for a company
8 that wants to -- even a company who hires people from the
9 outside and says what do we have to do, and they say you have
10 to do this, but I can't tell you what the FTC rules are
11 because they have never told anybody.

12 Again, I think the public is served by guiding
13 people beforehand rather than beating them after they --
14 after-hand. But the assistant director doesn't have the
15 authority to do that. He reports to the deputy director, who
16 reports to the director, who reports to the commission. So
17 he's way down in the pecking order.

18 So I understand what this witness said.

19 I suspect that this witness will say that he never
20 consulted with LabMD before about their security
21 processes. He's just come in to opine on the opinions
22 offered by Ms. Hill. Is that correct?

23 THE WITNESS: Correct.

24 THE COURT: I kind of wish he had been there
25 before.

1 One thing I do know is agencies that say you pay
2 for somebody to come in to look at your security practices
3 and this is what an expert said we had to do and needed to
4 do, that they have a different approach, because that's a
5 defense.

6 But if you want to cross-examine him, now is your
7 time. I had my say.

8 MR. GORJI: Your Honor, the government has no
9 cross.

10 THE COURT: So nothing further from Mr. Baker?
11 We appreciate your testimony.

12 THE WITNESS: Thank you very much.

13 THE COURT: You may step down.

14 Do you have any other witnesses or evidence you
15 want to present?

16 MR. RAIDER: Not at this time, Your Honor, no.

17 THE COURT: Anything the FTC wants to present?

18 MS. FASCETT: Assuming that you are not asking for
19 any argument on the jurisdictional issues, no, nothing
20 further to present. Thank you.

21 THE COURT: Anything else that LabMD wants to say?

22 MR. RUBINSTEIN: Your Honor, it's been extensively
23 briefed. If you have any questions, we are glad to answer
24 them. Other than that, we have nothing further.

25 THE COURT: All right. I will take it under

1 advisement.

2 And if there is nothing else to cover today or to
3 present, we will be in recess.

4 MR. RAIDER: Your Honor, just one quick point
5 before we go to recess?

6 Was Exhibit 14 admitted into evidence? That's the
7 Monday, January 6th, 2014, letter? If so, we would like to
8 tender it into evidence.

9 THE COURT: Well, did you tender it?

10 MR. RAIDER: I thought I did.

11 THE COURT: Did you object to it?

12 MR. GORJI: We didn't object, Your Honor.

13 THE COURT: I guess it's in.

14 MR. RAIDER: Thank you, Your Honor.

15 THE COURT: Which is, by the way, what my records
16 reflect was that it was tendered and not objected to and it
17 had been admitted, so you didn't really need to do that. But
18 now it's clear to everybody.

19 MR. RAIDER: Thank you.

20 THE COURT: All right. Now we will be in
21 recess.

22 (Proceedings adjourn at 11:46 a.m.)

23

24

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C E R T I F I C A T E

UNITED STATES OF AMERICA :
:
NORTHERN DISTRICT OF GEORGIA :

I, Nicholas A. Marrone, RMR, CRR, Official Court Reporter of the United States District Court for the Northern District of Georgia, do hereby certify that the foregoing 98 pages constitute a true transcript of proceedings had before the said Court, held in the city of Atlanta, Georgia, in the matter therein stated.

In testimony whereof, I hereunto set my hand on this, the 7th day of May, 2014.

/s/ Nicholas A. Marrone

NICHOLAS A. MARRONE, RMR, CRR
Registered Merit Reporter
Certified Realtime Reporter
Official Court Reporter
Northern District of Georgia

RX553

CENTERS FOR MEDICARE & MEDICAID SERVICES
CLINICAL LABORATORY IMPROVEMENT AMENDMENTS
CERTIFICATE OF COMPLIANCE

LABORATORY NAME AND ADDRESS

LAB MD, INC
2030 POWERS FERRY ROAD SUITE 520
ATLANTA, GA 30339

CLIA ID NUMBER

11D1016172

EFFECTIVE DATE

11/13/2011

LABORATORY DIRECTOR

USHA R VASA

EXPIRATION DATE

11/12/2013

Pursuant to Section 353 of the Public Health Services Act (42 U.S.C. 263a) as revised by the Clinical Laboratory Improvement Amendments (CLIA), the above named laboratory located at the address shown hereon (and other approved locations) may accept human specimens for the purposes of performing laboratory examinations or procedures.

This certificate shall be valid until the expiration date above, but is subject to revocation, suspension, limitation, or other sanctions for violation of the Act or the regulations promulgated thereunder.



Judith A. Yost

Judith A. Yost, Director
Division of Laboratory Services
Survey and Certification Group
Center for Medicaid and State Operations

If you currently hold a Certificate of Compliance or Certificate of Accreditation, below is a list of the laboratory specialties/subspecialties you are certified to perform and their effective date:

<u>LAB CERTIFICATION (CODE)</u>	<u>EFFECTIVE DATE</u>
BACTERIOLOGY (110)	08/24/2005
ROUTINE CHEMISTRY (310)	08/24/2005
ENDOCRINOLOGY (330)	08/24/2005
HISTOPATHOLOGY (610)	11/13/2003
CYTOLOGY (630)	11/13/2003
CYTOGENETICS (900)	05/24/2005

LAB CERTIFICATION (CODE) EFFECTIVE DATE



FOR MORE INFORMATION ABOUT CLIA, VISIT OUR WEBSITE AT WWW.CMS.HHS.GOV/CLIA OR CONTACT YOUR LOCAL STATE AGENCY. PLEASE SEE THE REVERSE FOR

LABMD - SUPP. PROD. YOUR STATE AGENCY'S ADDRESS AND PHONE NUMBER.

PLEASE CONTACT YOUR STATE AGENCY FOR ANY CHANGES TO YOUR CURRENT CERTIFICATE.

0113

4/30/15

CLIA ID Number: 11D1016172

LAB MD, INC
2030 POWERS FERRY ROAD SUITE 520
ATLANTA, GA 30339

STATE AGENCY ADDRESS AND PHONE NUMBER:

GA DHR/OFFICE OF REGULATORY SERVICES
DIAGNOSTIC SERVICE UNIT/CLIA
2 PEACHTREE ST NW 31-447
ATLANTA, GA 30303-3142
(404)657-5447

LABORATORY MAILING ADDRESS:

LABMD - SUPP. PROD.

0114

4/30/15

RX554



CIVIL INVESTIGATIVE DEMAND
Documentary Material

1. TO The Privacy Institute C/O Jim Kelly or Rian Wroblewski 1 Regency Court Marlton, New Jersey 08053	2. FROM UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION
--	---

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

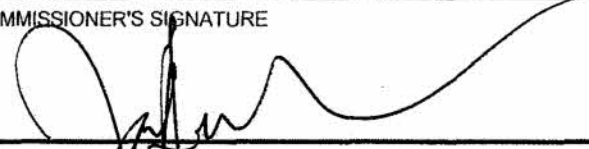
3. SUBJECT OF INVESTIGATION

See attached Resolutions

You are required by this demand to produce all documentary material in the attached schedule that is in your possession, custody or control, and to make it available at your address indicated above for inspection and copying or reproduction.

4. DATE AND TIME MATERIAL MUST BE AVAILABLE <p style="text-align: center;">AUG 13 2009</p>	5. COMMISSION COUNSEL Alain Sheer, Division of Privacy and Identity Protection Federal Trade Commission 601 N.J. Ave. N.W. Washington, D.C. 20580 (202.326.3321)
--	--

6. RECORDS CUSTODIAN Alain Sheer, Division of Privacy and Identity Protection Federal Trade Commission 601 N.J. Ave. NW (Stop NJ 3158) Washington, D.C. 20580	7. DEPUTY RECORDS CUSTODIAN Katrina Blodgett, Division of Privacy and Identity Protection Federal Trade Commission 601 N.J. Ave. NW (Stop NJ 3158) Washington, D.C. 20580
---	---

DATE ISSUED <p style="font-size: 2em;">7/10/09</p>	COMMISSIONER'S SIGNATURE 
---	--

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documentary material in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances relating to such production. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

Form of Certificate of Compliance*

I/We do certify that all of the documents required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this CID has not been submitted, the objection to its submission and the reasons for the objection have been stated.

Signature _____

Title _____

Sworn to before me this day

Notary Public

*In the event that more than one person is responsible for submitting documents responsive to this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY
AND/OR DATA SECURITY**

File No. P954807

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.


Donald S. Clark
Secretary

Issued: January 3, 2008

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NON-PUBLIC INVESTIGATION OF UNNAMED PERSONS, PARTNERSHIPS, CORPORATIONS AND OTHERS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF TITLE V OF THE GRAMM-LEACH-BLILEY ACT AND/OR SECTION 5 OF THE FTC ACT

File No. 0023284

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in acts or practices in violation of Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827 and/or Section 5 of the FTC Act, 15 U.S.C. § 45. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory process available to it be used in connection with this investigation for a period not to exceed three (3) years from the date of issuance of this resolution. The expiration of this three (3) year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the three (3) year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after expiration of the three (3) year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; and FTC Procedures and Rules of Practice, 16 C.F.R. § 1.1 *et seq.*, and supplements thereto.

By direction of the Commission.



Donald S. Clark
Secretary

Issued: July 21, 2006

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS:

Robert Pitofsky, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION INTO THE ACTS AND PRACTICES OF UNNAMED PERSONS,
PARTNERSHIPS AND CORPORATIONS ENGAGED IN ACTS OR PRACTICES IN
VIOLATION OF 15 U.S.C. § 1681 ET SEQ. AND/OR 15 U.S.C. § 45

File No. 992-3120

Nature and Scope of Investigation:

An investigation to determine whether persons, partnerships or corporations may be engaging in, or may have engaged in, acts or practices in violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and/or Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended, relating to information furnished to consumer reporting agencies, maintained in the files of consumer reporting agencies, or obtained as a consumer report from a consumer reporting agency. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

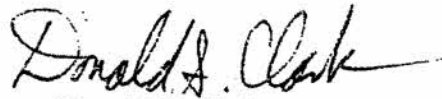
The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. § § 46, 49, 50 and 57b-1, as amended; FTC Procedures and Rules of Practices 16 C.F.R. 1.1 et seq. and supplements thereto.

Title VI of the Consumer Credit Protection Act, Section 621, 15 USCA § 1681s.

By direction of the Commission.


Donald S. Clark
Secretary

Dated: April 15, 1999

**Civil Investigative Demand
Schedule for Documentary Material**

To: The Privacy Institute
C/O Jim Kelly or Rian Wroblewski
1 Regency Court
Marlton, New Jersey 08053

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

- A. **“And,”** as well as **“or,”** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in the Schedule all information that otherwise might be construed to be outside the scope of the specification.
- B. **“Any”** shall be construed to include **“all,”** and **“all”** shall be construed to include **“any.”**
- C. **“CID”** shall mean this Civil Investigative Demand, the attached Resolutions, and the accompanying Schedule, including the Definitions, Instructions, and Specifications.
- D. The **“Company”** shall mean The Privacy Institute, its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants and other persons working for or on behalf of the foregoing.
- E. **“Document”** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, taped, recorded, filmed, punched, computer-stored, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book, opened electronic mail, and computer material (including print-outs, cards, magnetic or electronic tapes, discs and such codes or instructions as will transform such computer materials into easily understandable form).
- F. **“Each”** shall be construed to include **“every,”** and **“every”** shall be construed to include **“each.”**

- G. **“FTC”** or **“Commission”** shall mean the Federal Trade Commission.
- H. **“Identify”** or **“the identity of”** shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable.
- I. **“Personal information”** shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) medical information, such as medication, dosage, and diagnoses, physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) federal, state and local income tax filings; (j) a biometric record; (k) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (l) any information that is combined with any of (a) through (k) above. For the purpose of this definition, a “consumer” shall include an “employee,” and an individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, or independent contractor.
- J. **“Referring to”** or **“relating to”** shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.
- K. **“You”** and **“Your”** shall mean the person or entity to whom this CID is issued.

II. INSTRUCTIONS

- A. **Confidentiality:** This CID relates to an official, nonpublic, law enforcement investigation currently being conducted by the Federal Trade Commission. You are requested not to disclose the existence of this CID until you have been notified that the investigation has been completed. Premature disclosure could impede the Commission’s investigation and interfere with its enforcement of the law.
- B. **Applicable Time Period:** Unless otherwise directed in the specifications, the applicable time period for the request shall be from January 1, 2008 until the date of full and complete compliance with this CID.
- C. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim

of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, and date of the item;
2. the names, addresses, positions, and organizations of all authors and recipients of the item; and
3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

- D. Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. See 15 U.S.C. § 50; see also 18 U.S.C. §§ 1505, 1519.
- E. Petitions to Limit or Quash:** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).
- F. Modification of Specifications:** If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with Alain Sheer, at 202.326.3321. All such modifications must be agreed to in writing. 16 C.F.R. § 2.7(c).
- G. Certification:** A duly authorized manager of the Company shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.
- H. Scope of Search:** This CID covers documents in your possession or under your actual or constructive custody or control including, but not limited to, documents in the possession, custody, or control of your attorneys, accountants, directors, officers, and

employees, whether or not such documents were received from or disseminated to any person or entity.

- I. **Document Production:** You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Alain Sheer, Division of Privacy and Identity Protection, Federal Trade Commission, 601 N.J. Ave. N.W. (Stop NJ 3158), Washington, D.C. 20580. Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS. Notice of your intention to use the alternative method of compliance shall be given by mail or telephone to Alain Sheer, at 202.326.3321, at least five days prior to production.
- J. **Document Identification:** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. In addition, number by page all documents in your submission, and indicate the total number of documents in your submission. Also, number all media in your submission which contain ESI, and identify the file path where each of the individual files is located.
- K. **Production of Copies:** Unless otherwise stated, legible photocopies may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of original documents may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request.
- L. **Submission of Electronically Stored Information (“ESI”):** The following guidelines refer to any ESI you submit. But, before submitting any ESI, you must confirm with the FTC that the proposed formats and media types that contain such ESI will be acceptable to the government.
 1. Magnetic and other electronic media types accepted
 - (a) CD-R CD-ROMs formatted to ISO 9660 specifications.
 - (b) DVD-ROM for Windows-compatible personal computers.
 - (c) IDE and EIDE hard disk drives, formatted in Microsoft Windows-compatible, uncompressed data.

Note: Other types of tape media used for archival, backup or other purposes such as 4mm & 8mm DAT and other cassette, mini-cartridge, cartridge, and DAT/helical scan tapes, DLT or other types of media will be accepted only with prior approval.

2. File and record formats

- (a) E-mail: The FTC accepts MS Outlook PST files, MS Outlook MSG files and Lotus Notes NSF files. Any other electronic submission of email accepted only with prior approval.
- (b) Scanned Documents: Image submissions accepted with the understanding that unreadable images will be resubmitted in original, hard copy format in a timely manner. Scanned Documents must adhere to the following specifications:
 - (i) All images must be multi-page, 300 DPI - Group IV TIFF files named for the beginning bates number.
 - (ii) If the full text of the Document is available, that should be provided as well. The text should be provided in one file for the entire Document or email, named the same as the first TIFF file of the Document with a *.TXT extension.

Note: Single-page, 300 DPI – Group IV TIFF files may be submitted with prior approval if accompanied by an acceptable load file such as a Summation or Concordance image load file which denotes the appropriate information to allow the loading of the images into a Document management system with all Document breaks (document delimitation) preserved. OCR accompanying single-page TIFF submissions should be located in the same folder and named the same as the corresponding TIFF page it was extracted from, with a *.TXT extension.

- (c) Other ESI files: The FTC accepts word processing Documents in ASCII text, WordPerfect version X3 or earlier, or Microsoft Word 2003 version or earlier. Spreadsheets should be in MS Excel 2003 (*.xls) version or earlier. Database files should be in MS Access 2003 or earlier. PowerPoint presentations may be submitted in MS PowerPoint 2003 or earlier. Other proprietary formats for PC files should not be submitted without prior approval. Files may be submitted using the compressed ZIP format to reduce size and ease portability. Adobe Acrobat PDF (*.pdf) may be submitted where the normal business practice storage method is PDF.

Note: Database files may also be submitted with prior approval as

delimited ASCII text files, with field names as the first record, or as fixed-length flat files with appropriate record layout. For ASCII text files, field-level documentation should also be provided and care taken so that delimiters and quote characters do not appear in the data. The FTC may require a sample of the data to be sent for testing.

3. Security

- (a) All submissions of ESI to the FTC must be free of computer viruses. In addition, any passwords protecting Documents or files must be removed or provided to the FTC.
- (b) Magnetic media shall be carefully packed to avoid damage and must be clearly marked on the outside of the shipping container:

**MAGNETIC MEDIA – DO NOT X-RAY
MAY BE OPENED FOR POSTAL INSPECTION.**

III. SPECIFICATIONS FOR DOCUMENTARY MATERIAL

- 1. Produce documents sufficient to: identify non-governmental entities (without regard to type of business or industry) of which you are aware that have experienced peer-to-peer network file-sharing breaches of personal information (defined in Definition I, above); and describe in detail the nature and scope of each such breach. The response should include, but not be limited to, documents (such as a spreadsheet if one exists) that set out:
 - (a) the name of the entity;
 - (b) the name of each file shared by the entity; and
 - (c) for each such file:
 - (i) the number of unique individuals whose personal information is contained in the file;
 - (ii) the types of personal information contained in the file (by, for example, providing the first page of the file, including field names but redacting personal information about specific individuals);
 - (iii) the period of time during which the file was accessible on peer-to-peer networks;
 - (iv) the number of locations where the file is or was accessible on these networks; and

- (v) the number of times the file has been shared on these networks.
2. Produce documents sufficient to: identify all peer-to-peer file-sharing breaches experienced by Rite Aid Corporation; and describe in detail the nature and scope of each such breach. The response should include, but not be limited to, documents (such as a spreadsheet if one exists) that set out:
- (a) the name of each file shared by Rite Aid Corporation, if any; and
 - (b) for each such file:
 - (i) the number of unique individuals whose personal information is contained in the file;
 - (ii) the types of personal information contained in the file (by, for example, providing the first page of the file, including field names but redacting personal information about specific individuals);
 - (iii) the period of time during which the file was accessible on peer-to-peer networks;
 - (iv) the number of locations where the file is or was accessible on these networks; and
 - (v) the number of times the file has been shared on these networks.
3. Produce documents sufficient to: identify all peer-to-peer file-sharing breaches experienced by Walgreen Company; and describe in detail the nature and scope of each such breach. The response should include, but not be limited to, documents (such as a spreadsheet if one exists) that set out:
- (a) the name of each file shared by Walgreen Company, if any; and
 - (b) for each such file:
 - (i) the number of unique individuals whose personal information is contained in the file;
 - (ii) the types of personal information contained in the file (by, for example, providing the first page of the file, including field names but redacting personal information about specific individuals);
 - (iii) the period of time during which the file was accessible on peer-to-peer networks;

- (iv) the number of locations where the file is or was accessible these networks;
and
 - (v) the number of times the file has been shared on these networks.
- 4.
- (a) Produce documents sufficient to identify executable files for any malicious code or software you have captured while assessing peer-to-peer network file-sharing breaches, and produce a copy of each such file;
 - (b) produce documents sufficient to: identify the sources of the executable files provided in response to subpart (a) of this specification; and describe the circumstances of how each was obtained, including, but not limited to, any URL, IP address, date, or other information associated with the collection of each file; and
 - (c) produce copies of all documents reflecting reports, analyses, or the results of tests demonstrating that anti-virus programs do not detect the presence of such malicious software.
- 5.
- (a) Produce documents sufficient to identify executable files for any peer-to-peer applications that scan and index any or all information during the installation process without the consent of the user or that surreptitiously index and share files, and produce a copy of each such file; and
 - (b) produce documents sufficient to: identify the sources of the executable files provided in response to subpart (a) of this specification; and describe the circumstances of how each was obtained, including, but not limited to, any URL, IP address, date, or other information associated with the collection of each file.

RX615

Kelly, Andrea

From: Vandecar, Kim
Sent: Friday, July 11, 2014 6:23 PM
To: 'Shannon.Weinberg@mail.house.gov'; 'paul.nagle@mail.house.gov'
Cc: 'Kirby.Howard@mail.house.gov'; Oxford, Clinton P.
Subject: Fw: QFRs for Data Security Hearing House Subcommittee on Commerce.docx
Attachments: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Follow Up Flag: Follow up
Flag Status: Flagged

[Final FTC QFR's on data security](#)

From: Vandecar, Kim
Sent: Friday, July 11, 2014 02:28 PM
To: Howard, Kirby (Kirby.Howard@mail.house.gov) <Kirby.Howard@mail.house.gov>
Subject: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Kirby,

Can you use this version instead please?

Thanks,

Kim

Additional Questions for the Record
 Subcommittee on Commerce, Manufacturing, and Trade
 “Protecting Consumer Information: Can Breaches Be Prevented?”
 February 5, 2014

The Honorable Lee Terry

1. You testified that legislation would “strengthen [FTC’s] existing authority governing data security standards.” If you already have the authority to pursue data security enforcement actions now, why do you need a new law? What would change with such a law?

The Commission has authority to challenge companies’ data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases.

The Commission supports federal legislation that would (1) strengthen its existing tools to address companies’ inadequate practices for securing consumers’ data and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Such legislation is important for a number of reasons. First, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Second, enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology when implementing the legislation.

2. You testified that “although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring...consumers are protected.” Does that mean you believe preemption is appropriate in this area?

The Commission has expressed support for a federal data security and breach notification law that would preempt state law, but only if such a standard is sufficiently strong and the states are given the ability to enforce the law. If a consistent nationwide standard came at the expense of weakening existing state legal protections for consumers’ information, the Commission would not support the law.

3. You testify the Commission supports a Federal law that requires companies “in appropriate circumstances,” to provide notification to consumers. Can you describe what “appropriate” circumstances are? Are there occasions where notification could cause unnecessary problems for consumers and should not occur (e.g., cancelling a credit card when no account information was compromised)?

It is important for both consumers and businesses that the trigger for breach notification is balanced. We want to ensure that consumers learn about breaches that could result in identity theft, fraud, or other harm so they can take steps to protect themselves, but we do not want to notify consumers when the risk of harm is negligible,

as over-notification could cause consumers to become confused or to become numb to the notices they receive.

The following standard strikes the right balance: When an entity discovers a breach of security, the entity should be required to notify every consumer whose personal information was, or there is a reasonable basis to conclude was, accessed by an unauthorized person, unless the entity can demonstrate that there is no reasonable risk of identity theft, fraud, or other harm. (Of course, breach notification would only be triggered if specified categories of personal information have been the subject of a breach.) This standard balances the need for consumers to know when their information has been breached against the threat of over-notification for breaches that have no reasonable risk of harm.

4. You testify the Commission has settled 50 cases against businesses that it charged with failure to provide reasonable and appropriate protections for consumers' personal information. That does not include non-profits because the FTC's jurisdiction does not extend to those entities. With regard to data security, should the Commission have authority over non-profits? We have heard of universities and colleges suffering data breaches. Are they a common source of data breaches?

Yes, the Commission believes it should have jurisdiction over non-profits in this area. A substantial number of reported breaches have involved non-profit universities and health systems. Enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

5. Has the Commission pursued any data security cases that resulted in litigation instead of a settlement?

Most companies have chosen to settle the Commission's data security claims. However, the Commission currently has two data security cases in active litigation. *FTC v. Wyndham Worldwide Corp.* is pending in the federal district court in the District of New Jersey.¹ The Commission also approved the filing of a case in the FTC's administrative court, *In the Matter of LabMD*.²

6. How does the FTC enforce its "unfairness" standard? What principles guide the FTC so that businesses know when they might run afoul of the unfairness standard?

A company's practices are unfair if they cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.³ In the Commission's data security cases, reasonableness is the lynchpin. In determining whether a company's

¹ *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J.).

² *LabMD, Inc.*, No. C-9357 (F.T.C. compl. filed Aug. 28, 2013), available at <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf>.

³ See 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

data security practices are reasonable the Commission considers: the sensitivity and volume of consumer information a business holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The reasonableness test is designed to be flexible; reasonable data security safeguards should be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

In addition to the more than 50 data security consent orders, which provide guidance to businesses about what constitutes reasonable security, the Commission also has published business guidance and educational materials about good data security practices for companies. We have emphasized a process-based approach that includes: designating a person to be responsible for data security; conducting risk assessments; designing a program to address the risks identified, including training, security and incident response; and monitoring the program and updating it as necessary.

7. Has the FTC ever suffered a data breach?

We are not aware of any successful intrusions or infiltrations into the FTC network. Like other federal agencies and companies in the private sector, we are constantly under attack, and we use defense-in-depth (meaning multiple layers of security controls, such as firewalls, anti-virus and anti-spam tools, internet filters), continuous monitoring, and other methods to protect our information systems and the data they contain.

8. You mentioned that more than 16 million Americans have been victims of identity theft. What counts as identity theft for this purpose? Does it include cases where someone else uses your credit card number even if you end up without any financial loss?

The figure cited in the Commission’s written testimony is from the Bureau of Justice Statistics report, “Victims of Identity Theft, 2012,” which is the most recent BJS study of identity theft victims.⁴ For the purposes of that report, identity theft victims are defined as persons age 16 or older who experienced one or more of the following incidents in 2012: unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account); unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account); or misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information). According to the report, direct and indirect identity theft losses amounted to approximately \$24.7 billion in 2012.

Fraud detection programs are not perfect, so consumers are not reimbursed for all fraudulent charges placed on their accounts. Even when victims are ultimately reimbursed for out-of-pocket financial losses from a breach, this does not mean that they did not experience other, non-compensated harms from the breach. Consumers affected by breaches should constantly monitor their financial accounts for unauthorized charges. If consumers discover such charges, they must notify their credit and debit card issuers, close accounts, cancel cards, and wait for new cards to arrive. For those consumers with automatic bill pay, they must alert companies about the new account numbers to prevent late fees and other charges. Victims of identity theft can spend months reporting instances of fraud to creditors and reporting bureaus to restore their credit. Victims are not compensated for the economic cost from these expenditures of time.

The Honorable Jan Schakowsky

1. On January 10, 2014, Target announced that certain customer information – separate from the payment card data already revealed to have been stolen – had also been taken during the breach of its network systems in November and December 2013. This information included names, mailing addresses, phone numbers or email addresses for up to 70 million individuals.
 - a. What are the top risks to consumers whose names and contact information are stolen, including those Target customers who are among the 70 million? Please list them.

Personal information that is non-financial still requires protection, because it can be used to perpetuate fraud and identity theft. For instance, bad actors can use email addresses to perpetrate phishing attacks, send spam, or target users for malware, the latter of which can be used to install keyloggers or other technology to capture even more personal information. Moreover, targeted fraud becomes increasingly effective

⁴ Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.

the more personal information a criminal has about a consumer. For example, many consumers still use their email address as a user name on accounts. That, along with access to other personal information, may increase the danger of a criminal being able to ascertain a password and access a financial or other account or to perpetrate identity theft.

- b. Members and witnesses at recent congressional hearings on commercial data breaches have discussed at length potential enhancements to payment card security technology, such as the implementation of chip-and-PIN systems. At the Subcommittee hearing on February 5, 2014 – while stressing that the Commission does not recommend any particular technology – you indicated that “we would support any steps that are taken at the payment card system end to protect or better protect consumer information.” I believe it is important for retailers, issuers, and the payment card industry to urgently work together to improve card security. However, even if all the stakeholders involved agree to make payment card data as secure as possible, am I correct to understand that it is your position that that Congress should still separately address the overall security of personal data, including non-financial data, collected or stored by commercial entities?

That is correct. The Commission is aware of this developing technology, and according to some reports, it should be a positive step toward strengthening payment card security. However, this technology does not protect other information, such as health information, location information, or SSNs.

All companies that collect and handle consumer information should be required to implement reasonable data security measures. Reasonableness is the appropriate standard because it allows a company flexibility to develop a data security program based on factors such as the sensitivity and volume of consumer information it holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

The Commission reiterates our call for data security and breach notification legislation that would: (1) give us the authority to obtain civil penalties, an important remedy for deterring violations; (2) enable the FTC to bring cases against non-profits, such as hospitals and educational institutions, where many breaches occur; and (3) providing rulemaking authority under the Administrative Procedure Act, enabling the FTC to respond to changes in technology when implementing the legislation.

I believe the breach of marketing data can be a serious threat to consumers. As I said in response to questioning at the Subcommittee’s hearing, names and contact information can be used in phishing and social engineering schemes to try to perpetrate identity theft – and while harm from payment card breaches tends to be acute, harm from non-financial breaches tends to linger. In short, identity theft lasts; with chronic effects on consumers that can cost them everything they own.

- c. Do you agree that a breach of names and contact information can have a serious long-term impact on consumers, if used to trick them to give up sensitive identity data? Please explain your answer.

Yes. As discussed above, such information can be used to perpetrate fraud and identity theft, which can have lasting impacts on consumers' credit scores, in addition to the economic value of time lost and possible financial loss.

- 2. On January 31, 2014, the FTC announced the 50th data security settlement in its program of enforcement against those who fail to reasonably protect consumers' personal information. These settlements have been used to protect millions of consumers from unfair or deceptive practices that leave at risk sensitive information like usernames and passwords, Social Security numbers, and health, financial, and children's data. I commend your dedication to this issue.

Yet, during questioning at the Senate Banking Committee hearing on this topic on February 3, 2014, a Senator pointed out that with so many data breaches each year, 50 cases since 2002 may be commendable, but it may not be enough.

- a. Of course, all breaches do not rise to the level of FTC action, but can you please illustrate how the FTC uses its current legal framework to help with general deterrence, and how authorization to the FTC of new authorities, such as rulemaking authority under the Administrative Procedure Act and broader civil penalty authority, would increase the FTC's ability to deter unfair or deceptive data security practices?

Since 2002, the FTC has brought a steady stream of data security cases – resulting in more than 50 consent orders, and we have also issued extensive consumer and business education materials. During much of this time, we have been the only federal agency sending the message to a wide range of businesses, both small and large, across many sectors, of the need to maintain reasonable security to protect consumer data. Our complaints provide examples of data security practices that did not meet our flexible reasonableness test, and our consent orders serve as templates for best practices for companies setting up and implementing successful information security programs. In addition, we issue extensive guidance for consumers and businesses – especially small businesses – about how to safeguard consumer data. I believe that collectively the FTC's work in this area has helped promote appropriate investment in infrastructure and personnel to address the security of consumer data.

But, plainly, more needs to be done, and a unanimous Commission has concluded that the time has come for Congress to enact strong federal data security and breach notification legislation. We currently lack authority under Section 5 to obtain civil penalties, which are critical to appropriate deterrence of lax security practices. Likewise, enabling the FTC to bring cases against non-profits, over which we presently lack authority, would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, APA rulemaking would give us flexibility in implementing the statute by

making changes where appropriate – for example, to the definitions – to respond to changes in technology and changing threats.

- b. Recent newspaper commentary has suggested that by seeking to strengthen its data security authority, the FTC is acknowledging that it currently lacks the authority to police companies' data security practices. How do you respond to such an assertion?

The Commission principally has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases to date. In fact, a federal district court recently affirmed the FTC's authority to use Section 5 in the data security area.⁵

The Commission has called for data security legislation that would strengthen its existing tools and authority to help us in this endeavor, namely, civil penalty authority, jurisdiction over non-profits, a nationwide breach notice requirement to be enforced by the FTC and the states, and APA rulemaking to ensure we have adequate flexibility to respond to new technology and threats in implementing the statute.

The Honorable Jerry McNerney

1. Thank you for your leadership within the FTC, especially with regards to the work that is being done on privacy issues. What sort of authority does the Commission have or need from Congress to institute nationwide breach notification processes?

The FTC has authority to investigate breaches and bring civil enforcement actions under Section 5 of the FTC Act for deceptive or unfair acts or practices – such as deceptively claiming to reasonably safeguard consumer data. We have authority to seek equitable remedies for violations of Section 5, which does not include civil penalties.⁶ The FTC also generally lacks authority to require companies to issue notification to affected consumers to alert them to a breach of their personal information (with the exception of our narrow scope of authority under the HI-TECH Act). We similarly lack authority over non-profits, which have been the source of a number of breaches. To remedy these gaps, a unanimous Commission has called on Congress to enact legislation to pass a nationwide breach notification law to apply to all companies under the FTC's jurisdiction – expanding that jurisdiction to include non-profits –and to give the Commission civil penalty authority and authority to flexibly respond to changes in technology in implementing the law via APA rulemaking.

2. Businesses are understandably leery of the idea of additional regulations, but many people that I have talked with agree that a national standard is easier to deal with than varying state standards when it comes to data breach notification rules. In your opinion, how can the FTC

⁵ See *F.T.C. v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *petition for leave to appeal filed* (3d Cir. July 3, 2014).

⁶ By contrast, the FTC has civil penalty authority under the Fair Credit Reporting Act for security violations by “consumer reporting agencies,” such as the national credit bureaus.

and Congress best work together to come up with a national standard that doesn't impose unfairly upon states' rights?

Breach notification and data security standards at the federal level, with appropriate preemption of state law as discussed below, would extend notifications to all citizens nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A federal law would create uniform protections for all American consumers. However, our support for a federal law that would preempt state law has been conditioned on both a standard that is sufficiently strong and on giving states the ability to enforce the law, an important role for state Attorneys General.

The Honorable Peter Welch

1. We've seen the FTC take a strong leadership position on many issues, not only bringing enforcement actions but also convening experts from industry and academia at workshops. These workshops have been valuable opportunities for the FTC to write reports on what it learns, including guidance to companies when appropriate. It seems to me like an annual workshop and report on data security would be valuable given the recent problems companies have been having -- can we expect the FTC to have such a workshop soon?

Thank you for your recognition of the FTC's leadership on many issues and the value of our use of enforcement actions and public workshops. As you may know, emerging areas in privacy and security are frequent subjects of FTC workshops, studies, and reports. For instance, in June of last year, we held a workshop on threats to mobile security, in which we convened a group of leading experts to discuss mobile malware, the role of platforms in security, and ways to improve security in the mobile ecosystem.⁷ Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy and security implications of a number of new technologies in the marketplace, including mobile device tracking, alternative scoring products, and apps and devices that collect consumer-generated health data.⁸ At the Commission's November 2013 conference on the Internet of Things, much of the discussion focused on security challenges presented by "smart" devices.⁹

Moreover, the FTC just published its first annual "Privacy and Data Security Update," which is an overview of the FTC's enforcement, policy initiatives, and consumer

⁷ See Mobile Security: Potential Threats and Solutions (June 4, 2013), *available at* <http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions>.

⁸ See FTC to Host Spring Seminars on Emerging Consumer Privacy Issues, *available at* <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues>.

⁹ See Internet of Things - Privacy and Security in a Connected World (Nov. 19, 2013), *available at* <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

outreach and business guidance in the areas of privacy and data security from January 2013-March 2014.¹⁰ We expect to update this document every year.

¹⁰ Federal Trade Commission Staff, 2014 Privacy and Security Update (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

RX616

Kelly, Andrea

From: Vandecar, Kim
Sent: Thursday, July 17, 2014 2:27 PM
To: 'will.wallace@mail.house.gov'; 'Michelle.Ash@mail.house.gov'
Subject: Fw: QFRs for Data Security Hearing House Subcommittee on Commerce.docx
Attachments: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Follow Up Flag: Follow up
Flag Status: Flagged

From: Vandecar, Kim
Sent: Wednesday, July 16, 2014 12:52 PM
To: Eichorn, Mark
Subject: FW: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Additional Questions for the Record
Subcommittee on Commerce, Manufacturing, and Trade
“Protecting Consumer Information: Can Breaches Be Prevented?”
February 5, 2014

The Honorable Lee Terry

1. You testified that legislation would “strengthen [FTC’s] existing authority governing data security standards.” If you already have the authority to pursue data security enforcement actions now, why do you need a new law? What would change with such a law?

The Commission has authority to challenge companies’ data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases.

The Commission supports federal legislation that would (1) strengthen its existing tools to address companies’ inadequate practices for securing consumers’ data and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Such legislation is important for a number of reasons. First, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Second, enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology when implementing the legislation.

2. You testified that “although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring...consumers are protected.” Does that mean you believe preemption is appropriate in this area?

The Commission has expressed support for a federal data security and breach notification law that would preempt state law, but only if such a standard is sufficiently strong and the states are given the ability to enforce the law. If a consistent nationwide standard came at the expense of weakening existing state legal protections for consumers’ information, the Commission would not support the law.

3. You testify the Commission supports a Federal law that requires companies “in appropriate circumstances,” to provide notification to consumers. Can you describe what “appropriate” circumstances are? Are there occasions where notification could cause unnecessary problems for consumers and should not occur (e.g., cancelling a credit card when no account information was compromised)?

It is important for both consumers and businesses that the trigger for breach notification is balanced. We want to ensure that consumers learn about breaches that could result in identity theft, fraud, or other harm so they can take steps to protect themselves, but we do not want to notify consumers when the risk of harm is negligible,

as over-notification could cause consumers to become confused or to become numb to the notices they receive.

The following standard strikes the right balance: When an entity discovers a breach of security, the entity should be required to notify every consumer whose personal information was, or there is a reasonable basis to conclude was, accessed by an unauthorized person, unless the entity can demonstrate that there is no reasonable risk of identity theft, fraud, or other harm. (Of course, breach notification would only be triggered if specified categories of personal information have been the subject of a breach.) This standard balances the need for consumers to know when their information has been breached against the threat of over-notification for breaches that have no reasonable risk of harm.

4. You testify the Commission has settled 50 cases against businesses that it charged with failure to provide reasonable and appropriate protections for consumers' personal information. That does not include non-profits because the FTC's jurisdiction does not extend to those entities. With regard to data security, should the Commission have authority over non-profits? We have heard of universities and colleges suffering data breaches. Are they a common source of data breaches?

Yes, the Commission believes it should have jurisdiction over non-profits in this area. A substantial number of reported breaches have involved non-profit universities and health systems. Enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

5. Has the Commission pursued any data security cases that resulted in litigation instead of a settlement?

Most companies have chosen to settle the Commission's data security claims. However, the Commission currently has two data security cases in active litigation. *FTC v. Wyndham Worldwide Corp.* is pending in the federal district court in the District of New Jersey.¹ The Commission also approved the filing of a case in the FTC's administrative court, *In the Matter of LabMD*.²

6. How does the FTC enforce its "unfairness" standard? What principles guide the FTC so that businesses know when they might run afoul of the unfairness standard?

A company's practices are unfair if they cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.³ In the Commission's data security cases, reasonableness is the lynchpin. In determining whether a company's

¹ *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J.).

² *LabMD, Inc.*, No. C-9357 (F.T.C. compl. filed Aug. 28, 2013), available at <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf>.

³ See 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

data security practices are reasonable the Commission considers: the sensitivity and volume of consumer information a business holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The reasonableness test is designed to be flexible; reasonable data security safeguards should be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

In addition to the more than 50 data security consent orders, which provide guidance to businesses about what constitutes reasonable security, the Commission also has published business guidance and educational materials about good data security practices for companies. We have emphasized a process-based approach that includes: designating a person to be responsible for data security; conducting risk assessments; designing a program to address the risks identified, including training, security and incident response; and monitoring the program and updating it as necessary.

7. Has the FTC ever suffered a data breach?

We are not aware of any successful intrusions or infiltrations into the FTC network. Like other federal agencies and companies in the private sector, we are constantly under attack, and we use defense-in-depth (meaning multiple layers of security controls, such as firewalls, anti-virus and anti-spam tools, internet filters), continuous monitoring, and other methods to protect our information systems and the data they contain.

8. You mentioned that more than 16 million Americans have been victims of identity theft. What counts as identity theft for this purpose? Does it include cases where someone else uses your credit card number even if you end up without any financial loss?

The figure cited in the Commission’s written testimony is from the Bureau of Justice Statistics report, “Victims of Identity Theft, 2012,” which is the most recent BJS study of identity theft victims.⁴ For the purposes of that report, identity theft victims are defined as persons age 16 or older who experienced one or more of the following incidents in 2012: unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account); unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account); or misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information). According to the report, direct and indirect identity theft losses amounted to approximately \$24.7 billion in 2012.

Fraud detection programs are not perfect, so consumers are not reimbursed for all fraudulent charges placed on their accounts. Even when victims are ultimately reimbursed for out-of-pocket financial losses from a breach, this does not mean that they did not experience other, non-compensated harms from the breach. Consumers affected by breaches should constantly monitor their financial accounts for unauthorized charges. If consumers discover such charges, they must notify their credit and debit card issuers, close accounts, cancel cards, and wait for new cards to arrive. For those consumers with automatic bill pay, they must alert companies about the new account numbers to prevent late fees and other charges. Victims of identity theft can spend months reporting instances of fraud to creditors and reporting bureaus to restore their credit. Victims are not compensated for the economic cost from these expenditures of time.

The Honorable Jan Schakowsky

1. On January 10, 2014, Target announced that certain customer information – separate from the payment card data already revealed to have been stolen – had also been taken during the breach of its network systems in November and December 2013. This information included names, mailing addresses, phone numbers or email addresses for up to 70 million individuals.
 - a. What are the top risks to consumers whose names and contact information are stolen, including those Target customers who are among the 70 million? Please list them.

Personal information that is non-financial still requires protection, because it can be used to perpetuate fraud and identity theft. For instance, bad actors can use email addresses to perpetrate phishing attacks, send spam, or target users for malware, the latter of which can be used to install keyloggers or other technology to capture even more personal information. Moreover, targeted fraud becomes increasingly effective

⁴ Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.

the more personal information a criminal has about a consumer. For example, many consumers still use their email address as a user name on accounts. That, along with access to other personal information, may increase the danger of a criminal being able to ascertain a password and access a financial or other account or to perpetrate identity theft.

- b. Members and witnesses at recent congressional hearings on commercial data breaches have discussed at length potential enhancements to payment card security technology, such as the implementation of chip-and-PIN systems. At the Subcommittee hearing on February 5, 2014 – while stressing that the Commission does not recommend any particular technology – you indicated that “we would support any steps that are taken at the payment card system end to protect or better protect consumer information.” I believe it is important for retailers, issuers, and the payment card industry to urgently work together to improve card security. However, even if all the stakeholders involved agree to make payment card data as secure as possible, am I correct to understand that it is your position that that Congress should still separately address the overall security of personal data, including non-financial data, collected or stored by commercial entities?

That is correct. The Commission is aware of this developing technology, and according to some reports, it should be a positive step toward strengthening payment card security. However, this technology does not protect other information, such as health information, location information, or SSNs.

All companies that collect and handle consumer information should be required to implement reasonable data security measures. Reasonableness is the appropriate standard because it allows a company flexibility to develop a data security program based on factors such as the sensitivity and volume of consumer information it holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

The Commission reiterates our call for data security and breach notification legislation that would: (1) give us the authority to obtain civil penalties, an important remedy for deterring violations; (2) enable the FTC to bring cases against non-profits, such as hospitals and educational institutions, where many breaches occur; and (3) providing rulemaking authority under the Administrative Procedure Act, enabling the FTC to respond to changes in technology when implementing the legislation.

I believe the breach of marketing data can be a serious threat to consumers. As I said in response to questioning at the Subcommittee’s hearing, names and contact information can be used in phishing and social engineering schemes to try to perpetrate identity theft – and while harm from payment card breaches tends to be acute, harm from non-financial breaches tends to linger. In short, identity theft lasts; with chronic effects on consumers that can cost them everything they own.

- c. Do you agree that a breach of names and contact information can have a serious long-term impact on consumers, if used to trick them to give up sensitive identity data? Please explain your answer.

Yes. As discussed above, such information can be used to perpetrate fraud and identity theft, which can have lasting impacts on consumers' credit scores, in addition to the economic value of time lost and possible financial loss.

- 2. On January 31, 2014, the FTC announced the 50th data security settlement in its program of enforcement against those who fail to reasonably protect consumers' personal information. These settlements have been used to protect millions of consumers from unfair or deceptive practices that leave at risk sensitive information like usernames and passwords, Social Security numbers, and health, financial, and children's data. I commend your dedication to this issue.

Yet, during questioning at the Senate Banking Committee hearing on this topic on February 3, 2014, a Senator pointed out that with so many data breaches each year, 50 cases since 2002 may be commendable, but it may not be enough.

- a. Of course, all breaches do not rise to the level of FTC action, but can you please illustrate how the FTC uses its current legal framework to help with general deterrence, and how authorization to the FTC of new authorities, such as rulemaking authority under the Administrative Procedure Act and broader civil penalty authority, would increase the FTC's ability to deter unfair or deceptive data security practices?

Since 2002, the FTC has brought a steady stream of data security cases – resulting in more than 50 consent orders, and we have also issued extensive consumer and business education materials. During much of this time, we have been the only federal agency sending the message to a wide range of businesses, both small and large, across many sectors, of the need to maintain reasonable security to protect consumer data. Our complaints provide examples of data security practices that did not meet our flexible reasonableness test, and our consent orders serve as templates for best practices for companies setting up and implementing successful information security programs. In addition, we issue extensive guidance for consumers and businesses – especially small businesses – about how to safeguard consumer data. I believe that collectively the FTC's work in this area has helped promote appropriate investment in infrastructure and personnel to address the security of consumer data.

But, plainly, more needs to be done, and a unanimous Commission has concluded that the time has come for Congress to enact strong federal data security and breach notification legislation. We currently lack authority under Section 5 to obtain civil penalties, which are critical to appropriate deterrence of lax security practices. Likewise, enabling the FTC to bring cases against non-profits, over which we presently lack authority, would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, APA rulemaking would give us flexibility in implementing the statute by

making changes where appropriate – for example, to the definitions – to respond to changes in technology and changing threats.

- b. Recent newspaper commentary has suggested that by seeking to strengthen its data security authority, the FTC is acknowledging that it currently lacks the authority to police companies' data security practices. How do you respond to such an assertion?

The Commission principally has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases to date. In fact, a federal district court recently affirmed the FTC's authority to use Section 5 in the data security area.⁵

The Commission has called for data security legislation that would strengthen its existing tools and authority to help us in this endeavor, namely, civil penalty authority, jurisdiction over non-profits, a nationwide breach notice requirement to be enforced by the FTC and the states, and APA rulemaking to ensure we have adequate flexibility to respond to new technology and threats in implementing the statute.

The Honorable Jerry McNerney

1. Thank you for your leadership within the FTC, especially with regards to the work that is being done on privacy issues. What sort of authority does the Commission have or need from Congress to institute nationwide breach notification processes?

The FTC has authority to investigate breaches and bring civil enforcement actions under Section 5 of the FTC Act for deceptive or unfair acts or practices – such as deceptively claiming to reasonably safeguard consumer data. We have authority to seek equitable remedies for violations of Section 5, which does not include civil penalties.⁶ The FTC also generally lacks authority to require companies to issue notification to affected consumers to alert them to a breach of their personal information (with the exception of our narrow scope of authority under the HI-TECH Act). We similarly lack authority over non-profits, which have been the source of a number of breaches. To remedy these gaps, a unanimous Commission has called on Congress to enact legislation to pass a nationwide breach notification law to apply to all companies under the FTC's jurisdiction – expanding that jurisdiction to include non-profits –and to give the Commission civil penalty authority and authority to flexibly respond to changes in technology in implementing the law via APA rulemaking.

2. Businesses are understandably leery of the idea of additional regulations, but many people that I have talked with agree that a national standard is easier to deal with than varying state standards when it comes to data breach notification rules. In your opinion, how can the FTC

⁵ See *F.T.C. v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *petition for leave to appeal filed* (3d Cir. July 3, 2014).

⁶ By contrast, the FTC has civil penalty authority under the Fair Credit Reporting Act for security violations by “consumer reporting agencies,” such as the national credit bureaus.

and Congress best work together to come up with a national standard that doesn't impose unfairly upon states' rights?

Breach notification and data security standards at the federal level, with appropriate preemption of state law as discussed below, would extend notifications to all citizens nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A federal law would create uniform protections for all American consumers. However, our support for a federal law that would preempt state law has been conditioned on both a standard that is sufficiently strong and on giving states the ability to enforce the law, an important role for state Attorneys General.

The Honorable Peter Welch

1. We've seen the FTC take a strong leadership position on many issues, not only bringing enforcement actions but also convening experts from industry and academia at workshops. These workshops have been valuable opportunities for the FTC to write reports on what it learns, including guidance to companies when appropriate. It seems to me like an annual workshop and report on data security would be valuable given the recent problems companies have been having -- can we expect the FTC to have such a workshop soon?

Thank you for your recognition of the FTC's leadership on many issues and the value of our use of enforcement actions and public workshops. As you may know, emerging areas in privacy and security are frequent subjects of FTC workshops, studies, and reports. For instance, in June of last year, we held a workshop on threats to mobile security, in which we convened a group of leading experts to discuss mobile malware, the role of platforms in security, and ways to improve security in the mobile ecosystem.⁷ Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy and security implications of a number of new technologies in the marketplace, including mobile device tracking, alternative scoring products, and apps and devices that collect consumer-generated health data.⁸ At the Commission's November 2013 conference on the Internet of Things, much of the discussion focused on security challenges presented by "smart" devices.⁹

Moreover, the FTC just published its first annual "Privacy and Data Security Update," which is an overview of the FTC's enforcement, policy initiatives, and consumer

⁷ See Mobile Security: Potential Threats and Solutions (June 4, 2013), *available at* <http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions>.

⁸ See FTC to Host Spring Seminars on Emerging Consumer Privacy Issues, *available at* <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues>.

⁹ See Internet of Things - Privacy and Security in a Connected World (Nov. 19, 2013), *available at* <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

outreach and business guidance in the areas of privacy and data security from January 2013-March 2014.¹⁰ We expect to update this document every year.

¹⁰ Federal Trade Commission Staff, 2014 Privacy and Security Update (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

RX644

RX 644

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

STAFF REPORT



TIVERSA, INC.: WHITE KNIGHT OR HI-TECH PROTECTION RACKET?

**PREPARED FOR
CHAIRMAN DARRELL E. ISSA
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM**

**U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
JANUARY 2, 2015**

**EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD
WALLACE**

Table of Contents

I. *Introduction*..... 5

II. *Tiversa’s Scheme to Defraud the Congress and Executive Agencies* 6

III. *Tiversa’s Lack of Cooperation with this Investigation* 7

IV. *Tiversa, Inc.* 9

 A. Background on the company..... 9

 B. Tiversa’s claimed abilities to monitor and track files and users on the peer-to-peer network are exaggerated. 11

 C. The Marine One leak 16

 D. Boback created a hostile work environment at Tiversa 18

 E. Boback has not been forthcoming regarding the nature of his close relationship with Wallace, or the central role Wallace played at Tiversa 26

 F. Tiversa’s Unseemly Business Practices..... 39

 1. Tiversa used fearmongering tactics to generate business..... 39

 2. Tiversa systematically mined for files for “potential” clients as a solicitation tactic. 42

 3. Boback Misrepresented Howard Schmidt’s Role in Generating Business Contacts for Tiversa..... 47

 4. Boback Misrepresented Information about Tiversa’s Capabilities to Clients 52

V. *Tiversa’s Relationship with the Federal Trade Commission*..... 53

 A. Tiversa misrepresented the extent of its relationship with the FTC to the Committee.. 54

 B. The FTC misrepresented the extent of its relationship with Tiversa to the Committee. 56

 C. The FTC failed to question Tiversa’s creation of a dubious shell organization, the Privacy Institute, to funnel information to the FTC..... 58

 D. Tiversa manipulated advanced, non-public, knowledge of FTC regulatory actions for profit 62

 E. Information provided by Tiversa formed the basis of the FTC’s case against LabMD. 67

 F. Tiversa withheld documents from the FTC 72

VI. *Tiversa’s Involvement with House Ethics Committee Report Leak* 78

 A. The *Washington Post* breaks the story 78

 B. Tiversa “assists” the House Ethics Committee in its investigation..... 83

VII. *Open Door Clinic*..... 88

 A. Initial contact with Tiversa..... 89

B. Tiversa only provided self-serving information to the Open Door Clinic in July 2008 92

C. Tiversa facilitates a class action lawsuit against the Open Door Clinic, and contacts Open Door patients directly 93

D. Tiversa did not charge Bruzzese for the same information it refused to provide to the Open Door Clinic 97

E. Tiversa provided information on the Open Door Clinic to the FTC 98

VII. *Conclusion* 98

Key Findings

- Rather than the cyber “white knight” Tiversa purports to be, the company often acted unethically and sometimes unlawfully in its use of documents unintentionally exposed on peer-to-peer networks.
- At least one Tiversa employee, under the direction of CEO Robert Boback, provided intentionally false information to the United States government on more than one occasion. Boback later provided false testimony about fabricated documents to the U.S. House of Representatives.
- According to a whistleblower, Tiversa fabricated that an Iranian IP address downloaded and disclosed the blue prints for the President’s helicopter, Marine One. Tiversa allegedly did so in order to receive press attention for the company. The Committee found that statements made by Tiversa under oath about this matter could not be substantiated.
- After obtaining information on HIV/AIDS patients at a clinic in Chicago, Tiversa employees called the patients, purportedly in an attempt to get the clinic to hire Tiversa. When the clinic refused to hire Tiversa, the company gave the information to a lawyer that worked with the company who filed a class-action lawsuit that eventually settled for a substantial amount of money.
- Tiversa had information about a breach at the House Ethics Committee exposing information about investigations into Members of Congress. Tiversa did not return this information to the Ethics Committee and instead appears to have sought publicity for the leak.
- Tiversa’s co-founder claims the company is in possession of a greater quantity of sensitive and classified information than NSA-leaker Edward Snowden.
- Information provided by Tiversa to the FTC through a shell organization known as the Privacy Institute was only nominally verified but was nonetheless relied on by the FTC for enforcement actions.
- Tiversa obtained non-public, advanced knowledge of FTC enforcement actions from which it attempted to profit.
- According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography and classified government documents.

I. Introduction

In the summer of 2013, the Committee learned the Federal Trade Commission would bring an enforcement action against LabMD, a Georgia-based cancer screening company, under the guise of its authority under Section 5 of the FTC Act.¹ Serving as the basis for the enforcement action, the FTC filed an administrative complaint against LabMD after the personal information of approximately 9,000 LabMD patients was exposed on a peer-to-peer network.

Tiversa, a Pittsburgh-based company that sells peer-to-peer monitoring services, provided information on LabMD and nearly 100 other companies to the FTC. This information formed the basis for multiple enforcement actions and dozens of warning letters sent by the FTC. In August 2013, Mike Daugherty, LabMD's CEO, expressed concern to the Committee about both the relationship between the FTC and Tiversa, Inc., and the veracity of the information provided by Tiversa. In April of the following year, the Committee became aware of a former Tiversa employee with allegations of substantial misconduct related to Tiversa's dealings with the federal government.

Committee staff interviewed Tiversa's CEO, Robert Boback, on June 5, 2014. Boback's testimony failed to assuage Committee's concerns and instead raised many more questions about the relationship between Tiversa and various federal government agencies. Two days later, Boback was deposed for a second time in the FTC action against LabMD. There were several major inconsistencies between this testimony and the testimony he provided to the Committee only days earlier.²

During the course of this investigation, the Committee conducted ten day-long transcribed interviews and reviewed over 50,000 pages of documents. Documents and testimony obtained by the Committee in the course of its investigation displayed a troubling pattern with respect to Tiversa's business practices. Tiversa routinely provided falsified information to federal government agencies. Instead of acting as the "white knight" the company purports to be, Tiversa often acted unethically and sometimes unlawfully after downloading documents unintentionally exposed on peer-to-peer networks. At least one Tiversa employee, under the direction of Boback, provided intentionally false information to the United States government on more than one occasion. This is a crime. In addition, Boback provided false testimony about fabricated documents to the U.S. House of Representatives.

In many instances, documents that Tiversa produced to the Committee pursuant to a subpoena issued on June 3, 2014 lacked important context without explanation. Such gaps prompted the Committee to ask Tiversa's representatives on several occasions whether the company had produced all documents responsive to the Committee's subpoena as well as search terms proposed by Committee staff. Tiversa did not provide the Committee with assurances or a written statement that all documents had, in fact, been produced. Accordingly, the Committee sought to obtain additional information from third parties. These third parties provided a substantial number of documents to the Committee that Tiversa failed to produce. For example, Tiversa never produced documents showing it had advanced non-public knowledge of FTC

¹ Federal Trade Commission Act, 15 U.S.C. § 45 (2006).

² The Committee sent Boback a lengthy letter demanding explanations for the inconsistencies. Many questions posed in that letter remain unanswered.

enforcement actions and took steps to profit from that knowledge. The Committee also found that Tiversa withheld from the FTC a series of documents that are inconsistent with testimony company officials provided under oath. Tiversa's lack of cooperation with this investigation, and the withholding of key documents from the FTC, lead the Committee to believe that Tiversa has not produced all relevant documents responsive to this Committee's subpoena.

According to the testimony of a whistleblower and documents obtained in this investigation, Tiversa appears to have provided intentionally false information to this Committee and numerous other federal departments and agencies. Tiversa has further used and overstated its relationships with Congress and federal agencies to advance its unethical business model. The Committee's findings should give pause to any government entities which have relied or are planning to rely on information provided by Tiversa.

II. Tiversa's Scheme to Defraud the Congress and Executive Agencies

Several years ago, Tiversa CEO Robert Boback began perpetrating a scheme in which at least one Tiversa employee manipulated documents legitimately found on the peer-to-peer network to show that the documents had spread throughout the peer-to-peer network. For example, Tiversa downloaded a file that computer A shared on a peer-to-peer network. The file could be copied and the metadata easily manipulated thoroughly widely-accessible computer software programs to make it appear that it had been downloaded by computers B, C, and D, and thus spread throughout the peer-to-peer network. Tiversa relied on the manipulated documents to create a need for their "remediation" services and to grow the company's reputation through press statements and manipulation of media contacts. Boback told media contacts that certain documents, including sensitive government documents, spread throughout the peer-to-peer network when in fact they had not.

According to a whistleblower, Tiversa not only provided the manipulated information to its clients, but in some instances also provided false documents to various entities of the United States government, including the Congress and several agencies. Not only is this unethical, but it is illegal to give false information to the United States government.³ It is also illegal to obstruct a congressional investigation by providing false information to a congressional committee.⁴

³ See 18 U.S.C. § 1001, which states in pertinent part:

[W]hoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully . . . makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under this title, imprisoned not more than 5 years. . . .

⁴ See 18 U.S.C. § 1505, which states in pertinent part: 18 U.S.C. § 1505 states, in pertinent part:

Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress—

Throughout this investigation, the Committee routinely found that information provided by Tiversa either could not be verified, or simply did not make sense. Part of the story always seemed to be missing. The whistleblower's testimony that Tiversa routinely falsified documents, however, filled in these gaps.

III. *Tiversa's Lack of Cooperation with this Investigation*

Over the course of this investigation, Tiversa failed to provide full and complete information to the Committee. On multiple occasions, the company received documents from third parties witnesses responsive to the Committee's subpoena and other document requests, but not produced by Tiversa.

The Committee issued a subpoena to Tiversa on June 3, 2014. The subpoena requested documents responsive to eleven different requests, including:

1. All documents and communications referring or relating to work performed by Tiversa, Inc. on behalf of, in conjunction with, or provided to, any department, agency, or other instrumentality of the U.S. Government.
2. All documents and communications referring or relating to work Tiversa, Inc. performed for the Federal Trade Commission.

* * *

4. All documents and communications referring or relating to internet protocol addresses that Tiversa, Inc. provided to any department or agency of the U.S. Government.

* * *

7. All documents and communications referring or relating to LabMD, Inc.⁵

Tiversa failed to fully comply with the subpoena. A third-party witness provided numerous documents to the Committee in which Tiversa discussed information it provided to the FTC, and knowledge it had of upcoming FTC enforcement actions, with that third-party. Tiversa failed to produce these documents to the Committee despite their clear responsiveness to the subpoena.

Tiversa withheld additional relevant documents responsive to subpoenas issued by the Committee and the FTC from both entities. In October 2014, Tiversa filed a Notice of

Shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.

⁵ H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014) [hereinafter Tiversa OGR subpoena].

Information in the LabMD FTC proceeding.⁶ Tiversa included two e-mails from 2012 as exhibits to the Notice of Information, claiming that the e-mails demonstrate that Wallace could not have fabricated the IP addresses in question. Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission to the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. Tiversa has not explained how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information supporting their position that the documents undermine what they assume to be Wallace's testimony.

Tiversa further failed to fully respond to a subpoena issued by the Federal Trade Commission. As discussed in more detail below, the FTC served Tiversa with a subpoena for documents related to its administration action against LabMD, a Georgia-based medical testing laboratory.⁷ Among other categories of documents, the subpoena requested "all documents related to LabMD."⁸ In responding to the subpoena, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

Finally, after the Committee learned of Tiversa's involvement with the Open Door Clinic, an AIDS clinic servicing low-income patients outside of Chicago, Tiversa produced selected documents about its involvement with the Open Door Clinic. Committee staff requested specific additional information, including any forensic analysis done by Tiversa of the Open Door Clinic files. Tiversa, through its attorneys, told the Committee that it only analyzed one of the numerous files that it found on the peer-to-peer network about the Open Door Clinic.⁹ In fact, as discussed below Tiversa provided extensive forensic services, including two versions of a forensic report, free of charge to Michael Bruzzese. Bruzzese filed a lawsuit against the Open Door Clinic after receiving information from Tiversa. Tiversa never produced the reports to the Committee. Tiversa's withholding of these reports in the face of a direct request from the Committee, and its false claim that it did not analyze most of the Open Door files, is unacceptable.

Given these numerous instances in which Tiversa failed to fully provide information to the Committee and the FTC, the Committee strongly believes that Tiversa may be withholding additional relevant documents. Tiversa's failure to produce numerous relevant documents to this Committee and the FTC, at a minimum, demonstrates a lack of good faith. At worst, Tiversa intentionally withheld documents and other information in the face of multiple subpoenas. Either way, Tiversa's actions call into question the credibility of the company and its CEO, Robert Boback, as a source of information for the FTC.

⁶ Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014) [hereinafter Notice of Information]. Chief Administrative Law Judge D. Michael Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose." Order on Respondent's Motion to Strike, In the Matter of Lab MD, Inc., No. 9357 (Nov. 19, 2014).

⁷ Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC subpoena].

⁸ *Id.*

⁹ Letter from Reginald J. Brown and Madhu Chugh, Wilmer Hale, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2014).

Boback created a culture of intimidation at Tiversa. The Committee has unfortunately learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormely accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.¹⁰ Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. The suit against Wallace effectively questions Mr. Wallace's Constitutional right to speak with Congress after the Committee approached him with questions related to allegations about Tiversa. These are clear instances of witness intimidation and interference with a congressional investigation on the part of Boback and Tiversa.

IV. *Tiversa, Inc.*

A. Background on the company

Robert "Bob" Boback and Samuel Hopkins founded and incorporated Tiversa, Inc., a privately-held corporation headquartered in Pittsburgh, Pennsylvania, in January 2004.¹¹ Prior to joining Tiversa, Boback was a practicing chiropractor who dabbled in other activities including buying and selling residential properties and selling cars on eBay.¹² Hopkins, a high-school dropout, wrote the source code for the proprietary technology that Tiversa later patented.¹³ Hopkins sold his shares in Tiversa for approximately \$3.5 million and left the company in 2011.¹⁴ Boback is currently the Chief Executive Officer.¹⁵

Tiversa promotes itself as a company of "cyberintelligence experts."¹⁶ The company maintains an impressive roster of Advisory Board members, including retired General Wesley Clark; Howard Schmidt, the former Cyber-Security Coordinator for President Obama and previously for President Bush; and Maynard Webb, the former CEO of eBay.¹⁷ The Advisory Board met on one occasion in January 2006.¹⁸

According to Tiversa's website, the company "provides P2P Intelligence services to corporations, government agencies and individuals based on patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day. Requiring no software or

¹⁰ E-mail from Dwight Bostwick, Att'y for Christopher Gormley, to H. Comm. on Oversight & Gov't Reform Majority Staff (Nov. 20, 2014, 4:40 p.m.).

¹¹ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback (June 5, 2014), at 7 [hereinafter Boback Tr.].

¹² *Id.* at 7.

¹³ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Samuel Hopkins (July 29, 2014), at 115, 56 [hereinafter Hopkins Tr.]; Boback Tr. at 56.

¹⁴ *Id.* at 8.

¹⁵ Boback Tr., at 8.

¹⁶ Tiversa, Company Overview, <http://www.tiversa.com/about/> (last visited Sept. 15, 2014).

¹⁷ *Id.*

¹⁸ Boback Tr. at 29.

hardware, Tiversa can locate exposed files, provide copies, determine file sources and assist in remediation and risk mitigation.”¹⁹

On July 24, 2007, during the tenure of Chairman Henry Waxman, Boback testified at a hearing before this Committee titled, “Inadvertent File Sharing Over Peer-to-Peer Networks.”²⁰ Boback’s 2007 testimony focused on the “privacy and security threats [that] are caused by inadvertent misuse of P2P file sharing software,” and his company’s work in this area.²¹ On July 29, 2009, when Rep. Edolphus Towns served as Committee Chairman, Boback again testified about Tiversa’s work in the area of P2P filing sharing and data security breaches.²² One particular statement garnered a great deal of attention from Members of the Committee and the national media. Boback testified:

In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.²³

During this hearing, Boback also provided information on files Tiversa obtained from numerous other companies and non-profit groups, including the Open Door Clinic that Tiversa had “discovered” on the peer-to-peer network.²⁴

According to a customer presentation document, Tiversa began working with U.S. government in the spring of 2004. Tiversa claims to have worked “exclusively with the CIA, DoD, DHS, FBI, JCS, and USAF regarding the disclosure of CLASSIFIED [*sic*] information.”²⁵ In reality, Tiversa may not have worked with some of these agencies at all. With others, its relationships were extremely minimal. Overall, the company’s claims are overstated.

From 2008 to 2009, Tiversa frequently contacted non-client companies whose documents it discovered on peer-to-peer networks. Under a “duty of care” policy, Tiversa notified companies whose information they found on peer-to-peer networks, and provided them with examples of the exposed documents.²⁶ Boback explained that by providing this information, Tiversa was essentially providing a public service. In practice, however, Tiversa provided very minimal information to the affected companies. The Committee’s investigation found that Tiversa typically provided one document. Even though Tiversa’s systems automatically captured other relevant information, such as the IP address from which the

¹⁹ *Id.*

²⁰ Peer-to-peer networks are often referred to as “P2P” networks.

²¹ *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov’t Reform*, 110th Cong. (2007) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.).

²² *Inadvertent File Sharing Over Peer-to-Peer Networks: How It Endangers Citizens and Jeopardizes National Security*, 111th Cong. (2009) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.).

²³ *Id.*

²⁴ *Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security: Hearing Before the H. Comm. on Oversight & Gov’t Reform*, 111th Cong. at 12 (July 29, 2009) (testimony of Robert Boback, CEO of Tiversa, Inc.).

²⁵ [TIVERSA-OGR-0021275].

²⁶ Hopkins Tr., at 205-06.

document was shared, Tiversa would not provide this information to a company unless it purchased Tiversa's services.

During the course of this investigation, the Committee spoke with several companies that chose not to hire Tiversa. In addition, the Committee located one company that did enter into a contract with Tiversa. Tiversa told the company that it spent a great deal of time "investigating" the source of the peer-to-peer leak, at high cost to the company. It appears, however, that Tiversa only provided information its systems automatically downloaded, such as the IP address that leaked the documents.²⁷ Tiversa further represented to this company that, in order to identify whether any of its computers had peer-to-peer software, it would have to access the company's network remotely and run a search. Tiversa lacks the capability to access a client's network remotely. In this instance, it seems likely that it "identified" the computer using peer-to-peer software by simply looking at the IP address of the computer that shared the confidential document. When the Committee asked Tiversa about its ability to remotely access client computer, Tiversa responded that it never made such a claim to any client.²⁸

In his transcribed interview, Samuel Hopkins described Tiversa as "a highly ethical company."²⁹ After a lengthy investigation, the Committee believes otherwise.

B. Tiversa's claimed abilities to monitor and track files and users on the peer-to-peer network are exaggerated.

Tiversa's business model relies on technology developed by Hopkins, including its trademarked and patented Eagle Vision X1 and Covio. Tiversa claims to have the ability to provide "true cloud security" by seeing the entire peer-to-peer network."³⁰ Further, Tiversa states that its technologies can "detect and record user-issued P2P searches, access and download files available on the P2P networks, determine the actual disclosure source of documents, track the spread of files across the entire P2P networks [*sic*], and remediate P2P file disclosures."³¹

Tiversa claims that its technology "enables us to view the entire network and thus provide real-time, actionable information regarding sensitive file disclosures related to your organization."³² In 2007, Boback's written testimony submitted to the House Oversight Committee summarized Tiversa's technological capabilities. Boback wrote:

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, **Tiversa can see the P2P network in its entirety in real time.**

²⁷ Briefing by Company A to H. Comm. on Oversight & Govt' Reform (July 16, 2014).

²⁸ Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 2, 2014).

²⁹ Hopkins Tr.at 54.

³⁰ Tiversa Learning Ctr., *Key Concepts*, <http://www.tiversa.com/learningcenter/resources/keyconcepts/>.

³¹ Marine One forensic report, pg. 2.

³² Tiversa Learning Ctr., *FAQ/Misconceptions*, <http://www.tiversa.com/learningcenter/resources/faq/>.

With this platform, **Tiversa has processed as many as 1.6 billion P2P searches per day**, more than the number of web searches entered into Google per day.³³

It is disputed, however, how many files Tiversa downloads daily off the peer-to-peer network. According to Jason Schuck, Tiversa downloads “maybe a million” files daily.³⁴ However, according to Boback, Tiversa downloads “the equivalent of the Library of Congress every three or four days.”³⁵ The Library of Congress is the largest library in the world, with more than 158 million items, including more than 36 million books and other print materials, 3.5 million recordings, 13.7 million photographs, 5.5 million maps, 6.7 million pieces of sheet music, and 69 million manuscripts.³⁶ In essence, Tiversa claims to be able to see the entire peer-to-peer network, instead of a smaller subset as seen by an individual user.

At the time of the leaks discussed in this report, Tiversa used generic and client-specific search terms, such as “reports,” “credit card,” or “secrets” to query the peer-to-peer network.³⁷ Even Tiversa analysts could not explain exactly how Eagle Vision keyed into the terms to download them into the data store; that is, analysts did not know definitively whether any document was in the data store due a search term hitting on the file’s name, for instance; the search term in the body of the file; or the search term in the name of a folder containing the file. Keith Tagliaferri, Tiversa’s Senior Vice President of Operations, and the individual in charge of Tiversa’s analytical work, stated:

I’m not well versed enough on the technology and how it works to know exactly how things key off and what could have downloaded this and that.

I’m aware of all different types of scenarios that can happen as far as why and when we download files. You know, one is matching a key term within a file title. Another is matching a key term within the content of a file.

I’ve read research that indicates that a folder name can hit on a file. So, for example, if you have a folder called “Work” and somebody searches for “Work,” the results that come back are all of the files that are within that folder.

There’s also a concept of browse host on peer-to-peer that I’m not sure if our systems have the ability to do or not. But you can literally go to an IP once you find one file and hit “Browse Host” and download all the files from that IP.

³³ *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov’t Reform*, 110th Cong., at 20 (2007) (written statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.) (emphasis added)

³⁴ H. Comm. on Oversight & Gov’t Reform, Transcribed Interview of Jason Schuck, at 12 (Aug. 1, 2014) [hereinafter Schuck Tr.]

³⁵ Boback Tr. at 143.

³⁶ Library of Congress, Fascinating Facts, <http://www.loc.gov/about/fascinating-facts/> Fascinating Facts (last accessed Dec. 22, 2014).

³⁷ Hopkins Tr. at 74.

So there's all kinds of different scenarios that can occur to cause files to be downloaded. I'm not well versed enough on the technical side of our systems to know exactly what would trigger files to be downloaded.³⁸

To Tagliaferri's knowledge, there was no way to verify by what search term a document was found and downloaded into the data store.³⁹

Tiversa's data store collects and accumulates all the information that is found by Eagle Vision; no documents are deleted.⁴⁰ Information enters Tiversa's data store, or repository of databases, in two ways. Either Tiversa's Eagle Vision software downloads the information from the peer-to-peer network, or the information is found independently from Eagle Vision and "injected" into the data store through an application called the Data Store Importer. Schuck described the application in the following way:

Q. So analysts have the ability to, I guess, inject files into the data store using the Data Store Importer program?

A. Correct.⁴¹

* * *

Q. How does it -- if I'm an analyst and I have a file that I want to put into the data store using this program, do you know what steps I take to do that?

A. Sure. If the file is in the correct format, you would place it in a pickup folder.

Q. What does it mean to have a file in the correct format?

A. So depending on the IP address that it was downloaded from, that would be prepended to the original file name.

Q. Who prepends the IP address?

A. Again, you're talking about for the Data Store Importer, right?

Q. Yes.

A. That would be whoever's bringing it in.

³⁸ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Keith Tagliaferri, at 106-07 (June 17, 2014) [hereinafter Tagliaferri Tr.].

³⁹ *Id.* at 107.

⁴⁰ *Id.* at 88-89.

⁴¹ Schuck Tr. at 19.

- Q. Are you aware of specific occasions on which the data store importer was used by analysts to put files into the data store?
- A. No, not offhand. That's, again, that's even though I oversee that, I'm not the one that's actually doing that. That would be the analyst.
- Q. To your knowledge, has the Data Store Importer been used to put files into the data store?
- A. I would assume so, yeah.⁴²

Eagle Vision directly downloads documents that either directly hit on a Tiversa search term, or are related to a Tiversa search term (i.e., other documents shared by a user also sharing a document that hits on a search term).⁴³ According to Hopkins, the creator of the technology, the system does not distinguish between downloaded and injected files.⁴⁴ Tiversa, through its attorneys, stated that analysts can “usually” tell if a file is downloaded or injected, but did not explain how its analysts can make that determination.⁴⁵ This distinction is critically important, as it would aid in understanding more fully Tiversa’s actions.

Tiversa’s Covio system indexes the IP address of all files it downloads from the peer-to-peer network. Every time a document containing a search term is shared on the peer-to-peer network, Tiversa’s system downloads the document and indexes it according to the IP address from which it was downloaded. Even if the document is exactly the same, the system will automatically re-download it and index it with the new IP address.⁴⁶ In this way, Tiversa can determine if a file is spreading, or being shared, throughout the peer-to-peer network.

Boback, however, has offered the Committee conflicting information about whether Tiversa’s technology actually does have the capability to automatically download and index documents as they spread throughout the peer-to-peer network. For example, according to Boback, Tiversa never downloaded a copy of a document belonging to LabMD, a cancer screening company, from one of LabMD’s computers in Georgia.⁴⁷ This document is at the heart of an ongoing FTC action against LabMD. Yet, the document hit on a search term provided by a client, and Tiversa does claim to have downloaded the file from several other IP addresses because of the search term.⁴⁸ Tiversa has never been able to explain to this Committee why its systems did not automatically download the file from LabMD but did download the document from so many other IP addresses. Either Tiversa’s technology can not do what Boback and Hopkins claim it can do, or Boback provided false information to the FTC and this Committee about Tiversa’s downloading of the LabMD document.

⁴² Schuck Tr. at 20-21.

⁴³ Hopkins Tr. at 43.

⁴⁴ *Id.* at 75.

⁴⁵ Letter from Reginald Brown, Att’y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov’t Reform (Sept. 2, 2014).

⁴⁶ Hopkins Tr. at 40.

⁴⁷ *Id.*; see also Tiversa, Forensic Investigation Report – LABMD0001 (June 4, 2014).

⁴⁸ Boback Nov. 2013 FTC Tr. at 41 (“I never downloaded the file from them. They only responded to the hash match.”).

Further, Tiversa has not taken steps to screen for illegal content, such as child pornography, before it is downloaded into the data store. In fact, analysts say that it is entirely possible that child pornography is sitting in Tiversa's data store currently. According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography. Tagliaferri stated that he had "heard anecdotally that there may be child pornography" downloaded into the data store.⁴⁹ He explained that "as part of that information that's being pulled down, you know, I suppose anything -- anything could come back. You know, it could be Word documents. It could be .pdf's. It could be images. It could be, you know, whatever."⁵⁰

According to Tiversa, The system also "records all user-issued P2P searches," meaning that Tiversa can see a search and record it.⁵¹ Typically, Tiversa can only see the queried search, and cannot identify the user issuing the search. Under very narrow circumstances, Tiversa can determine the IP address of the user issuing a search. Hopkins described Tiversa's limited ability to identify the IP address issuing a search. He stated:

[The search request] goes to the first three people, they hand it to all the three people there, so it's three and then it's what, nine, so forth. But it only goes five hops. So the three people that I'm connected to, that's the first hop. . . . After five hops, it's dropped off the network. But if you're connected to the three people and the search is one hop away, then you know it came from one of the people you're connected to. But out of the 3,000 people, three people in a security world is nothing.⁵²

Thus Tiversa can only determine the IP address of a user issuing the search if Tiversa is one of the three users directly connected to the searcher.

Boback, however, has exaggerated Tiversa's ability to determine the user issuing a search over the years. In 2011, Tiversa claimed to have information that Wikileaks was obtaining information from peer-to-peer networks.⁵³ Boback claimed that "Wikileaks is doing searches themselves on file-sharing networks."⁵⁴ He continued, "It would be highly unlikely that someone else from Sweden is issuing those same types of searches resulting in that same type of information."⁵⁵ Boback further explained that in a one-hour period in February 2009, Tiversa detected four Swedish computers issue 413 searches.⁵⁶

As explained to the Committee by Hopkins, however, Tiversa can only identify the IP address and geographic location of a computer issuing a search if Tiversa is one of only three peer-to-peer users directly connected to that computer. Otherwise, Tiversa can only see the search request, and not the user or location of the user issuing the search. Given the limitations of Tiversa's technology, Boback's statements are very likely exaggerated, if not outright false.

⁴⁹ Tagliaferri Tr. at 90.

⁵⁰ *Id.* at 91.

⁵¹ *Id.* at 160.

⁵² *Id.* at 169.

⁵³ Michael Riley, *Wikileaks May have Exploited Music, Photo Networks to Get Data*, BLOOMBERG (Jan. 20, 2011) <http://www.bloomberg.com/news/2011-01-20/wikileaks-may-have-exploited-music-photo-networks-to-get-classified-data.html>.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

Tiversa also claims that it can “remediate” damage from a document leaked over the peer-to-peer network. Tiversa, however, cannot remove an exposed document from the peer-to-peer network. Instead, Tiversa is limited to sending take-down notices to the internet service provider of the IP address. The success of the take-down notices depends, in part, on the location of the ISP.⁵⁷

C. The Marine One leak

In early 2009, Tiversa’s reputation exploded when the company disclosed that it found blueprints for Marine One on a computer in Iran. A whistleblower stated to the Committee, however, that Tiversa only found on the blueprints on a government contractor’s computer. Tiversa then manipulated the document by prepinning an Iranian IP address to make it appear that the plans had been downloaded in Iran via the peer-to-peer network. At Tiversa’s request, the Committee spoke with multiple federal agencies involved in the investigation into the Marine One leak. The Committee reviewed documents provided by Tiversa, including a forensic report prepared by Tiversa in June 2014, and received briefings and documents from federal agencies involved in the government’s investigation of the leak.⁵⁸ The Committee found that statements made by Tiversa about the Marine One leak could not be substantiated.

On September 17, 2007, Tiversa “detected” the Marine One file as being shared on the peer-to-peer network. Tiversa’s Eagle Vision software did not download this file automatically. Instead, a Tiversa analyst found the file using a stand-alone computer to search the peer-to-peer network. Tiversa determined that a government contractor was sharing the document on a peer-to-peer network.⁵⁹ That a contractor inadvertently shared the document on the peer-to-peer network is not in dispute. Tiversa, however, additionally claimed that a computer located in Iran downloaded and shared the file. These explosive allegations garnered large amounts of publicity for the company.

Tiversa claims that on February 25, 2009, it found that an Iranian computer was in possession of the same Marine One blueprints previously shared by the government contractor. According to Tiversa’s forensic report, the Iranian computer disclosed the document on the peer-to-peer network between October 27, 2006 and February 25, 2009.⁶⁰ Thus, Tiversa conveniently found the document on the network the very last day it was made available by the Iranian computer. The fact that the Iranian computer ceased sharing the document made it next to impossible for any agencies Tiversa alerted after February 25 to determine whether that computer was in fact in possession of the Marine One file.⁶¹

⁵⁷ Tagliaferri Tr. at 120, 161.

⁵⁸ All information contained in this report was provided to the Committee in an open and unclassified setting.

⁵⁹ Forensic Report at 4.

⁶⁰ Forensic Report at 10.

⁶¹ If the computer was still sharing the file after Tiversa reported its purported discovery, then individuals investigating the leak could have determined whether the document was, in fact, sharing the file using the peer-to-peer network.

The Committee spoke with Tim Hall, a former NCIS employee who investigated the Marine One leak, on multiple occasions. Hall is now the Director of Government Services at Tiversa.⁶² Hall told the Committee that another federal agency verified the information provided by Tiversa about the Marine One leak—specifically, that another agency verified that the file was being shared by a computer with an Iranian IP address. Hall testified:

Q. And do you know if the information was verified by other task force members?

A. Yes.

Q. How do you know that?

A. Because we worked hand in hand with them daily, just multiple conversations.

Q. Were you ever told how the information was verified?

A. No.

Q. Was all information passed on to other task force members to be verified, to the best of your recollection?

A. Yes. Yes.⁶³

Tiversa's counsel also repeatedly told the Committee that the federal government verified the information Tiversa provided about an Iranian computer being in possession of the Marine One document. But that is simply not the case. The Committee learned from NCIS that the joint task force investigating the incident was only able to verify that the IP address provided by Tiversa was located in Iran.⁶⁴ The agents did not verify whether that computer actually possessed the Marine One file as this was outside the scope of the investigation.⁶⁵

Given the amount of time that has passed, it is not possible to verify today whether the Marine One file ever spread to a computer in Iran. The Committee has great doubts, however, about Tiversa's story. Tiversa discovering that the document had spread to Iran on the very last day that the Iranian computer allegedly disclosed the file is far too convenient. Further, the Iranian computer purportedly shared the computer for over two years before Tiversa located the file. According to Tiversa, the Iranian computer was in possession of the file in September 2007, when Tiversa initially found that a government contractor improperly shared the document. Yet, Tiversa did not locate the file on the Iranian IP address at that time.

⁶² H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Timothy Hall at 26 (Sept. 3, 2014) [hereinafter Hall Tr.].

⁶³ Hall Tr. at 25-26.

⁶⁴ Briefing by Naval Crim. Investigative Service to H. Comm. on Oversight & Gov't Reform Majority and Minority Staff (Sept. 5, 2014). In the course of the investigation, the Committee received a document from a Tiversa whistleblower listing hundreds of IP addresses in rogue nations around the world.

⁶⁵ *Id.*

Tiversa has also not been able to explain to the Committee how it finally learned in February 2009 that the file spread to the Iranian computer. A Tiversa analyst found the original file in 2007, meaning that either no word in the document hit on a Tiversa search term, or Eagle Vision did not download the document when it should have done so.⁶⁶ Given that Eagle Vision also did not download the document between September 2007 and February 2009, it would appear that no word in the document hit on a Tiversa search term.⁶⁷ So, what prompted Tiversa to search for the document again in late February 2009? That the document does not appear to have been downloaded by Eagle Vision makes the fact that Tiversa downloaded the document on the very last day it was shared by the Iranian computer even more fortuitous.

The story is complicated, to be sure. But Tiversa's complicated tale about this leak unwound when the Committee heard from a whistleblower. According to the whistleblower, Tiversa fabricated that the Iranian IP address downloaded and disclosed the Marine One file. Tiversa allegedly did so in order to receive press attention for the company. This is a very serious allegation—one outside the capabilities of the Committee to verify. If true, then Tiversa provided knowingly false information to numerous agents of the federal government, including this Committee, and wasted federal resources as numerous agencies investigated a fraudulent report. Additionally, the publicity associated with this breach allowed Tiversa to exaggerate the degree to which U.S. intelligence was vulnerable to P2P leaks and sell itself as the solution.

D. Boback created a hostile work environment at Tiversa

Not only does Boback appear to have routinely exaggerated the technological capabilities of Tiversa, but he also created a hostile work environment and retaliated against employees who questioned him. In fact, numerous witnesses put Boback at the center of a hostile work environment at Tiversa. One Tiversa employee stated that he “had significant concerns about [Boback’s] ability to execute his job as CEO.”⁶⁸ The employee brought his concerns to a board member, citing Boback’s role in the “creation of a toxic environment,” “certain bullying incidences,” and “certain practices that I thought were reckless or inappropriate.”⁶⁹ A faction of employees, led by Boback, frequently left work, offended other employees, and engaged in unprofessional behaviors, including carrying guns to work.

Boback left the office frequently, sometimes for multiple days. In one instance, in early 2008, Boback left with Richard Wallace, the Director of Special Projects at Tiversa, “to pick up

⁶⁶ As explained above in Section IV(B), Tiversa’s technology should download a document containing a search term each time it spreads throughout the peer-to-peer network. Here, the Iranian computer downloading and sharing the document would create a new document in the eyes of the Eagle Vision system. If the document contained a search term, then it should have been downloaded. If the document contained a search term but was not downloaded for some reason, then Tiversa’s software failed to operate as advertised.

⁶⁷ Given the magnitude of the discovery, the Committee does not understand why Tiversa would not input key terms from the Marine One document into its automatic download system. Given the gap in time between the discovery of the two documents, either Tiversa neglected to perform this basic task for a leak of great national security significance, or its systems failed to perform as advertised.

⁶⁸ H. Comm. on Oversight & Gov’t Reform, Transcribed Interview of Christopher Gormley, at 27 (July 14, 2014) [hereinafter Gormley Tr.].

⁶⁹ *Id.* at 27.

a car in Atlanta.”⁷⁰ They were scheduled to be gone for only a day, but were instead gone two days.⁷¹ A former Tiversa employee said that this was a frequent habit: “Mr. Boback would generally come in late in the morning and leave fairly early in the afternoon as well... I’m not sure where he was during those hours.”⁷²

Boback encouraged inappropriate banter and comments by employees that detracted from the professional atmosphere and mission of Tiversa. One former employee testified:

Q. I'd like to start with a little bit of follow-up from the last hour. You were discussing with my colleagues some joking emails, I guess, for lack of a better term, that Mr. Wallace sent, and I believe you described that there were many of these emails that were sent among a certain group of people. Is that accurate?

A. I wouldn't say so much many emails, but there was a lot of banter, I guess, orally. And I'd say there was a certain amount of that you'd expect, but some of it in this case was out of line for what I considered a company of what we were trying to create was.

Q. Was Mr. Boback ever involved in this banter?

A. Yes.

Q. Did he ever express that he felt the banter was not appropriate for the workplace?

A. No.

Q. Did he make joking comments along the same lines of what other employees were saying?

A. Yes.⁷³

Boback routinely made offensive remarks to Tiversa employees, creating an atmosphere of harassment and intimidation. One employee described described Boback’s inappropriate comments to the Committee:

A lot of, I guess, homosexual jokes, right? This or that. I mean, something akin to being in a junior high school playground, and it was fairly rampant, and it was just, you know, difficult to not engage in that... one particular story that I do remember is we had a company meeting. Well, I entered the company meeting, and one of the -- and I don't remember who -- made a remark to that effect, and everyone in the meeting laughed,

⁷⁰ *Id.* at 38.

⁷¹ *Id.* at 38.

⁷² *Id.* at 40.

⁷³ *Id.* at 79.

including Mr. Boback. It was clearly uncomfortable for many in the room. And I think, you know, those are the issues I was trying to convey to the board member, just that we can't have an environment like that in today's day and age, and that can we at least put some boundaries to that kind of behavior inside the office.⁷⁴

Gormley described another instance of Boback acting in an unprofessional manner :

I remembered receiving an email that copied a colleague of mine, Griffin Schultz, that said, you know, "Chris, you should get a job as a Presidential piss boy," which just out of, you know -- stated very clearly it was a joke, but he stated it, that I should get that kind of job.⁷⁵

* * *

Q. What did you understand him to mean by that phrase?

A. I don't know what was in Mr. Boback's mind when he made that, other than the email said what it said. The context was Mr. Schultz was trying to make an introduction to some congressional staffers or somebody that he had known in the past, and there may have been some mention of various roles, but not Presidential piss boy, but it may have been in the context of that. And then he said, Chris, that's a great job for you, Presidential piss boy, and Griffin Schultz was on that email as well me.

Q. Do you recall when that email was sent?

A. That would have been, I believe, April 2008. It was in 2008. I don't -- I think it's April.⁷⁶

Boback also referred to "teabagging" with Wallace and Hopkins while at work. One employee described conversations he overheard at the office:

I would be at my desk listening to them talk about playing Halo 3 and how they teabagged this person from Russia or this person from -- but it was extremely rampant to the point where it was very disruptive to the business. So that was one of the things I reported to the board member, to say we need to get them engaged back in the business, because, you know, they were needed for doing business, and I, again, didn't think that was an appropriate conversation for a work office.⁷⁷

⁷⁴ *Id.* at 79-80.

⁷⁵ *Id.* at 19-21.

⁷⁶ *Id.* at 57-58.

⁷⁷ *Id.* at 179-80.

Boback also condoned employees carrying and wielding firearms , and brought a gun himself to the office on multiple occasions. Transcribed interviews with Tiversa employees reflect that both Sam Hopkins, the co-founder of Tiversa, and Boback carried guns while at work at Tiversa. Sam Hopkins was aware that Boback carried a gun around at the office:

- Q. Did you ever see any other weapons in the office of any kind?
- A. Bob had a handgun that I saw a few times.
- Q. And did he show you the gun when he was in the office?
- A. In his office, yeah.
- Q. Why did he -- do you know why he showed you this gun or do you--
- A. You know, just two guys talking and he had known that I was carrying.⁷⁸

Keith Tagliaferri saw Boback “walk by with [a gun case],” although he did not look inside the case.⁷⁹ Christopher Gormley was also aware that Boback carried a gun at work. Boback even showed Gormley his gun:

- Q. And what was the context of the meeting at which Mr. Boback pulled out his revolver and showed it to you?
- A. He just came in. He'd come in a lot. I mean, his office was close to mine. And, I believe, that day -- and I can't be certain of this, but I'm pretty sure that he had taken a number of individuals from the company out to shop for guns at a gun store.
- Some people from the company actually departed for the afternoon, and I didn't know where they went. Which was a fairly common activity, that he would disappear for long periods of time. But this particular afternoon, I mean, that was my belief at the time, that they went to a gun store, and this may have been a purchase then. But it was showing me that he had purchased this or had this. I wasn't sure whether he actually got it at the gun store or not. But that activity occurred that day.
- Q. Do you recall approximately when this took place?
- A. Yes. Well, let me think. It would've been in the first quarter of 2008, maybe April.⁸⁰

⁷⁸ Hopkins Tr. at 150.

⁷⁹ Tagliaferri Tr. at 161-62.

⁸⁰ Gormley Tr. at 21-22.

Gormley also described Boback displaying his gun in an intimidating manner:

[] I would later discover that, I mean, **Mr. Boback, at least as far as my personal experience went, had certain bullying tendencies....**

On one occasion, he entered my office and, you know, sat at a desk in front of me and reached into his sock holster and pulled out a revolver and showed me its features and functions. And I thought that that was extremely surprising, that somebody would actually have a concealed weapon in the office and then pull it out to me. And I didn't feel like he was going to use it on me, but I thought, what are you doing with this and why are you showing it to me? And I thought that was -- that was one incident. That was pretty stark.⁸¹

Boback never revealed to the Committee that he brought a gun to work. He was quick to suggest, however, that Hopkins carried a gun to work, out of fear of Wallace:

[Hopkins] told me years ago, that he purchased a gun and a carry permit as protection against Mr. Wallace solely to protect -- as he felt scared for his physical existence against Mr. Wallace....⁸²

Gormley also had personal knowledge of Hopkins bringing a gun to work, including one incident when Hopkins pointed a gun at Gormley:

Q. You mentioned other Tiversa employees carried weapons in the office. Do you recall which employees did that?

A. Well, one incident I remember **Sam Hopkins had gone and pulled it out and pointed at me down a hallway.**

* * *

Q. Did you feel threatened when Mr. Hopkins pointed the gun at you down the hallway?

A. I didn't feel threatened at the time.

Q. Did Mr. Hopkins say anything when he pointed the weapon?

A. I don't remember him saying anything. It may have been the same day that Mr. -- they all went to the gun store, and I don't know if it occurred after or before Mr. Boback, so I may have been more sensitized to the fact that there were weapons in the office that day, silly as that sounds.⁸³

⁸¹ *Id.* at 18-19 (emphasis added).

⁸² Boback Tr. at 205

⁸³ Gormley Tr. at 76 (emphasis added).

Boback also brought swords to the office, and distributed swords to Tiversa employees. According to Schultz, “Bob would hand out a sword to each new employee that he thought represented their character... I believe mine was like a Marine sword or something based on my time at Wharton and a few other things that he thought fit my character... Someone else got the sword Gandalf carried in *The Lord of the Rings* because he thought it fit their [*sic*] personality.”⁸⁴

The Committee learned of one instance where an employee attempted to take action against Boback and his intimidation tactics. Gormley described a professional disagreement he had with Boback over handling a forensic analysis issue. In a response that the Committee has found to be typical, Boback sent Gormley a threatening e-mail. Gormley testified about the incident:

Mr. Boback and I had a dispute as to how to handle the scope of that particular exercise [regarding how narrow or broad search terms should be kept for a prospective client]. I don't think either one of us were right or wrong... I contended that we should provide the whole. He contended that we keep it more narrow.

We had a very stark disagreement on how to handle that...And this was a highly negative—well, a very stark email to this effect sent to me, as well as a phone call later that evening when I was at an event with my daughters at school. And he told me to keep it within the scope he told to me, to keep it, **or else there would be consequences—in other words, either terminations or significant consequences.**

[T]hat's what motivated me to go to Mr. Becker.

I was actually quite concerned to go to Mr. Becker because I feared retaliation.⁸⁵

From that point forward, Gormley chose not to confront Boback because he felt that it “usually wasn't very productive, because [Boback] would come at you and tuck it away as something that potentially could be used later.”⁸⁶

When Boback heard that a Tiversa employee had approached the board with concerns about his professionalism and leadership, he became irate and sought retaliation:

I was very concerned about retaliation or being—it turned out that the feedback I gave to Mr. Becker, I believe, was incorporated through various actions the board had taken... [T]here was a point in 2008, in September, early September, where Mr. Boback called me up and said he'd just received a review and some feedback from the board, and one of the elements was that an... employee in the company had given that [negative] feedback. And he was extremely angry about that and **wanted**

⁸⁴ Schultz Tr. at 112-13.

⁸⁵ Gormley Tr. at 25-26 (emphasis added).

⁸⁶ *Id.* at 30.

to know who that person was, and he was going to take whatever measures it took to find that out.

In the subsequent week and a half, **he held individual meetings with each person and also held a group meeting where he asked each person in the executive team, did you say it, did you say it?** And he suspected that [redacted name], an employee of the company, may have been the person. My guess is he also suspected me. I denied that at the time, out of concern for my own wellbeing I guess. But he wouldn't let it go.

* * *

He came into my office, everyone had left, shut the door, sat in the same seat that, you know, the pistol and everything had been pulled out, and basically kept asking me questions in different ways to see if it was me[.]

* * *

Now, he also said that... **he thought it was [redacted] and that I needed to fire [redacted] because he suspected that it was her.** [Redacted] happens to be a personal friend of mine, somebody I brought into the company. So I was in a very conflicted situation, because I either fire somebody that I know didn't do it or I admit that I did it. So I told Mr. Boback that it was me that evening and told him why, you know, went through some of the major reasons that I mentioned that I gave to Mr. Becker.

* * *

But, after that point, **there was a lot of fallout that I believe occurred because of that incident.** And it was a very difficult period for me personally at the time, **because at that point I was ostracized from the rest of the company,** had to apologize to different people within the company for having went [sic] out the chain of command and saying things, that, in Mr. Boback's view, weren't true.⁸⁷

Soon after, in September 2008, Gormley was demoted from COO to "Vice President of Data."⁸⁸ Boback explicitly told Gormley that the demotion was the "outcome [of] those discussions with the board."⁸⁹ Nonetheless, Gormley tried to perform his new job. Boback, however, refused to let Gormley succeed. Gormley testified::

This is in 2009, and as part of the data business, I was involved on a potential acquisition of the company by Experian. Mr. Boback and I got into an argument about how to interact with Experian in that discussion. I

⁸⁷ *Id.* at 31-32 (emphasis added).

⁸⁸ *Id.* at 33.

⁸⁹ *Id.* at 33-34.

wanted Lisa Frankovitch to be the person who would interact with Experian and then have Mr. Boback back her up in the discussions. He didn't agree.

We had a disagreement about that, and **subsequently he just said, "Joel wants you off the deal,"** meaning this board member wants me off the deal. This is subsequent to [the]... first board meeting, and I didn't believe that that was the case. I reached out to Lisa Frankovitch, who had that relationship, but then she suggested I talk to Joel directly. I called him up, and he indicated that **he never said that, and he said that I should go talk to Bob and make that clear.** So it was—at the time it clearly caught up with him, no, he didn't, Joel didn't actually state that. So that was one indication.⁹⁰

Gormley was terminated in late 2009, he believes in retaliation for reporting Boback to Tiversa's Board of Directors.⁹¹

Boback's intimidating comments did not end even after Gormley was fired:

Q. Have you had any other communication with Mr. Boback since your termination? I don't know if threats of litigation counts, but have you had any communication with Mr. Boback following your termination?

A. Yes. The points of communication after termination, I guess the first time he communicated with me, I decided not to sell some options that I owned in approximately 2011, and he sent me an email that started with "LOL, LOL, LOL." That means -- you guys know what that means -- "laugh out loud, laugh out loud." And **he ridiculed me for not selling my options and then made fun of my role as the director of downstream marketing and just sent that to me out of the blue.** And I still have that email. That was 2011.⁹²

The Committee has further learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormley accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.⁹³ Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. Such witness intimidation tactics are unacceptable.

⁹⁰ *Id.* at 89-90 (emphasis added).

⁹¹ *Id.* at 87-88.

⁹² Gormley Tr. at 147 (emphasis added).

⁹³ E-mail from Dwight Bostwick, Att'y for Christopher Gormley, to H. Comm. on Oversight & Gov't Reform Majority Staff (Nov. 20, 2014, 4:40 p.m.).

E. Boback has not been forthcoming regarding the nature of his close relationship with Wallace, or the central role Wallace played at Tiversa

In advancing the narrative that Wallace is the source of all of Tiversa's problems, Boback has repeatedly contradicted his own statements to the Committee. Often, instead of answering the question asked, he instead spoke tangentially about Wallace's bad character and dangerous propensities.

Tiversa recruited Wallace in mid-2007.⁹⁴ Wallace was given substantial responsibilities at Tiversa. In his professional duties, Wallace was tasked with "reflect[ing] the technology of Tiversa to customers when they would come in."⁹⁵ Wallace was "many times called out to be the expert technical person in the data store area of our office."⁹⁶ Wallace also was Tiversa's face for the FBI, and spent around 20-30% of his time "doing work related to the FBI arrangement."⁹⁷ A former Tiversa employee said that Boback "absolutely" trusted Wallace's work.⁹⁸

Boback would like the Committee to believe that Wallace was and continues to be the source of all of Tiversa's problems. If that were true, Boback would be in gross dereliction of his official duties as CEO of Tiversa. However, accounts of multiple Tiversa employees indicate that Boback and Wallace shared an exceedingly close relationship, and that Boback leveraged his status as CEO to manipulate Wallace to act on his behalf.

Numerous Tiversa employees have characterized Boback and Wallace as close, and testified that the two spent a great deal of time together. As one employee stated :

[T]hey were together constantly... Mr. Wallace tended to know where Mr. Boback was. If you needed to know where Mr. Boback was, you'd ask Rick, or Molly Trunzo would ask Rick, because many times he knew where Bob was.

* * *

I mean, my perception of Mr. Wallace was that he was Mr. Boback's spy. And I think one on one I had a decedent relationship with Mr. Wallace, but I think when he was in a group or he was with Mr. Boback, he became different, and he tried to show his worth, I think, in multiple ways with Mr. Boback.⁹⁹

Troublingly, numerous Tiversa employees described Boback and Wallace following cars together. Czarnecki stated that he heard "some kind of talk about [Boback or Wallace using a

⁹⁴ Gormley Tr. at 176-77.

⁹⁵ *Id.* at 50.

⁹⁶ *Id.* at 50.

⁹⁷ *Id.* at 86.

⁹⁸ *Id.* at 178.

⁹⁹ *Id.* at 48-49 (emphasis added).

GPS device] at the old offices”¹⁰⁰ to track a specific individual.¹⁰¹ Another former employee also heard Boback and Wallace talk about putting a tracking device on a vehicle.¹⁰² Gormley believed that he would be followed after he approached a board member with concerns about Boback’s professionalism, “because there was a history of Mr. Boback and Mr. Wallace following people for fun, you know. And so, in this instance, I felt like they may follow me and, you know, a retaliation may occur[.]”¹⁰³

Ultimately, statements made by Boback impugning Richard Wallace simply do not add up with the facts of Wallace’s employment while he was at Tiversa.

a. Wallace received only a glowing performance review while a Tiversa employee.

Wallace received one review during his tenure at Tiversa. This review, given in 2008, described Wallace as a talented analyst and consummate professional. Among his “key accomplishments,” the review stated that Wallace:

Led the work and served as an official informant to F.B.I. related to child pornography on P2P file sharing networks. Rick also managed the day-to-day relationships with two F.B.I agents. This work was new to Tiversa and Rick handled the many ambiguities associated with this work in a highly professional manner that was respected by his F.B.I. counterparts.¹⁰⁴

The review describes Wallace as “critical in aligning Tiversa for a potential deal with the Air Force Office of Special Investigation,” and “*instrumental* in a number of press events serving as an expert for reporter research.”¹⁰⁵ The review stated that as a cyber forensic analyst, Wallace “monitor[ed] accounts of Cigna, American Express, and PGP and [was] a core Cyber Forensic Analyst with, for example, University of Florida, Wagner, Wachovia, GE.” Wallace also “contributed insight into the design and operation of Tiversa F.A.S.T. productivity suite which when fully implemented should substantially improve CFA productivity.”

The review listed Wallace’s strengths as the following:

Work Ethic

Rick has an outstanding work ethic and can always be relied upon to put in the extra effort surrounding a project or finding files to support a Tiversa business opportunity. There have been many weekends and/or late nights where Rick has worked extra hours either in the office or at home to make Tiversa’s business objectives happen.

¹⁰⁰ H. Committee on Oversight & Gov’t Reform, Transcribed Interview of Orion Czarnecki, at 72 (Sept. 16, 2014) [hereinafter Czarnecki Tr.].

¹⁰¹ *Id.* at 72.

¹⁰² *Id.* at 40-41.

¹⁰³ Gormley Tr. at 26.

¹⁰⁴ Tiversa, 2008 Review of Richard Wallace (Aug. 4, 2008).

¹⁰⁵ *Id.* at 1 (emphasis in original).

Client and Media Relations

Rick has received exemplary feedback for his work from client contacts most notably from F.B.I. and Cigna. Rick has also managed relationships and provided P2P background to outside parties and media during their investigations of P2P risks.

Drive for new business / press

Rick is constantly scanning the P2P (literally) for files or individuals that will yield new Tiversa business, yield more tickets for existing Tiversa clients thus strengthening Tiversa's value with existing clients, and finding situations that put the P2P or Tiversa in a strong public relations position. Rick always seems to be able to find a hard hitting file or P2P situation to accelerate our client acquisition, existing relationships or to help serve as a nugget for a powerful news story. For example, recently Rick found a number of American Express internal files in the Philippians [*sic*] which have strengthened our relationship with Amex's CIO and put us in contact with Accenture.

Enthusiasm for the P2P Space

There is no other person at Tiversa that lives and breathes P2P more than Rick. His level of enthusiasm for finding P2p sourced information is contagious and extremely valuable to Tiversa.¹⁰⁶

Going forward, the review pointed to two areas in which Wallace could improve. First, the review suggested that Wallace “[c]onsider [d]ownstream [a]ffects [*sic*]” by

[N]ot only continu[ing] his outstanding work as an individual contributor, but [] seek[ing] to make the whole team more effective, more highly scalable, less Dilbert-like by balancing the short term needs for sales and files with the long term need to make everyone effective and ready to handle more scale. I would ask Rick to please provide me direct feedback on areas that he thinks can be more effective and to **take a leadership role** in addressing the issue.¹⁰⁷

Second, the review suggested that Wallace pursue searching other peer-to-peer networks for “veins’ of file gold”.¹⁰⁸

Rick is a maestro of LimeWire operation and sleuthing. The business benefits greatly every time we find more “veins” of file gold not only including sources on LimeWire, but on wholly new P2P networks. For instance, the addition of eDonkey to our roadmap was guided by the large magnitude of sensitive files that appeared by using the eMule client in

¹⁰⁶ *Id.* at 1-2.

¹⁰⁷ *Id.* at 2.

¹⁰⁸ *Id.*

Tiversa's lab. In between leveraging LimeWire for the benefits already highlighted above, I would like Rick to experiment with other clients to discover new caches of files and help guide our product roadmap.¹⁰⁹

In consideration of his performance, the review noted that Wallace was to be given a 9.8% raise, in addition to the 20.6% Wallace received at the end of 2007.¹¹⁰ The review concluded by congratulating Wallace on his achievements.¹¹¹

It is not clear who at Tiversa wrote Wallace's review. Gormley stated that he, Schultz, and Boback would have all had input on the review.¹¹² Although Schultz was Wallace's direct supervisor, and although Schultz reported to Gormley, Boback gave Wallace a direct raise without telling either of Wallace's supervisors.¹¹³ This caused Gormley to think that he, Schultz, and Boback "had split responsibilities for Mr. Wallace."¹¹⁴

Tiversa employees characterized their relationships with Wallace as typical professional relationship. Tagliaferri stated that he and other Tiversa employees socialized with Wallace:

Q. Did you socialize outside of the office with Mr. Wallace?

A. Sometimes. If he would have a bonfire or a Christmas party or something like that at his house then I would attend something like that.

Q. And were these events attended by Tiversa employees generally?

A. Sometimes. There might be, you know, a couple of other Tiversa employees there, and other professionals in the security industry that we all work with that may attend one of his get togethers.¹¹⁵

When asked to describe Wallace's professional contribution to Tiversa, Tagliaferri stated:

[Wallace] found a lot of information that was very sensitive, confidential and bad stuff out on these networks that shouldn't be out there, and he was really good at finding information out on the networks.

And, to that extent, you know, would we have found that information without Rick? I don't know. Maybe we would have. **But the things that Rick found certainly contributed to the company. He was an asset to the company to that extent.**¹¹⁶

¹⁰⁹ *Id.* at 2-3.

¹¹⁰ *Id.* at 3.

¹¹¹ *Id.*

¹¹² Gormley Tr. at 205.

¹¹³ Gormley Tr. at 55.

¹¹⁴ Gormley Tr. at 55.

¹¹⁵ Tagliaferri Tr. at 156.

¹¹⁶ Tagliaferri Tr. at 98 (emphasis added).

Boback and Wallace's relationship extended beyond the professional. When Boback and Wallace interacted in the office, it was not through the traditional hierarchical channels:

- Q. Mr. Boback was the CEO, correct?
- A. Yes.
- Q. And Mr. Wallace was an analyst, correct?
- A. Mr. Wallace was an information forensic engineer.
- Q. And so, in the corporate hierarchy, Mr. Boback was certainly above Mr. Wallace, correct?
- A. Yes, substantially.
- Q. Is the type of direction that Mr. Wallace took from Mr. Boback typical to the type of direction that other employees in Tiversa took from Mr. Boback? Or was there something different about the nature of the direction that Mr. Wallace was taking from Mr. Boback?
- A. It was much more one-on-one, less hierarchy involved. It wasn't like Mr. Boback went to me and then I went to Mr. Schultz and then Mr. Schultz went to Mr. Wallace to ask him to do something. **It was, "Hey, Rick, you're coming with me," and off he went. Or, "We don't know where Rick is. He's with Bob." It was much more direct. So it was independent of any kind of hierarchy that existed.**¹¹⁷

Another Tiversa employee verified that even though Wallace was a forensic security analyst, he reported directly to Boback.¹¹⁸ According to a former Tiversa employee, Boback and Wallace were very close, with Boback exerting greater influence over the relationship:

- Q. Would you describe them as close friends?
- A. Yeah, absolutely... **[T]here was nobody that was closer to Bob in the time frame that Rick was there than him**, with maybe the small exception of Mr. Hopkins, but even Mr. Hopkins had his own life, and he just wanted to go do his thing. Mr. Wallace and Mr. Boback were tied at the hip.

¹¹⁷ Gormley Tr. at 214-15 (emphasis added).

¹¹⁸ Tagliaferri Tr. at 75 ("[M]y understanding was that he reported to Mr. Boback.")

Q. You would say they're close friends?

A. Yeah, I would say that.

Q. **Would you describe one of them as having a dominant role in the friendship?**

A. **Yeah, Mr. Boback.**

Q. Could I ask why you would say that?

A. Well, Mr. Boback had a bigger house, he had all the little—you know, the toys and games, and so that would certainly lead the way, and just the way they interacted with one another. **It was clear that Mr. Wallace was taking direction from Mr. Boback, not the other way around.**¹¹⁹

Boback, on the other hand, has consistently mischaracterized Wallace and his responsibilities to the Committee. When asked a simple question about what duties Wallace performed at Tiversa, Boback could not give a straight answer:

Q. Okay. When Mr. Wallace was employed at Tiversa, which section or sections did he work in?

A. I don't know that he necessary -- he really didn't work in -- he was never a cleared individual, so he never had the clearance portion of it when everyone else went through there. **Mr. Wallace's role at Tiversa was regarding, or most of his work was child pornography,** searching for child pornography and providing it as a confidential informant to the FBI, and also identifying new cyber risks for, you know, educational purposes that he would then provide to me and then whenever I would go, I've traveled around the country training law enforcement for FBI LEEDA, L-E-E-D-A and he would sometimes travel with me and, you know, highlight different risks for the cyber world that law enforcement wouldn't see otherwise.¹²⁰

* * *

Q. Was Mr. Wallace first hired as an analyst?

A. Yes, he was.

¹¹⁹ Gormley Tr. at 180 (emphasis added).

¹²⁰ Boback 62-63 (emphasis added).

- Q. And when was he first hired by Tiversa as an analyst?
- A. I'm not sure exactly, but I think in 2007, maybe. I'm not sure of the exact date, but the summer roughly, I think I remember around the summer of 2007.
- Q. Was Mr. Wallace first hired for his skills as an analyst or for his work with the FBI?
- A. No, Mr. Wallace was hired as an analyst. Mr. Wallace was a stay-at-home dad in Illinois and his wife was in the military, and Mr. Wallace ran a Web site called SeeWhatYouShare.Com. Essentially, See What You Share, what he did was, he would search for files leaked or exposed on file-sharing networks and he would publish them on his Web site. Essentially, he was the first iteration of WikiLeaks, but he did it under the SeeWhatYouShare.com website.

So an individual, Tom Sydnor, Thomas Sydnor who used to work at -- work with Senator Hatch in the Senate Judiciary, Tom Sydnor told me about this Richard Wallace and said, hey, you should talk to this guy because he's, you know, in the space that you're in where no one knows anything, he's doing some searches that may be of interest to you, and he said, he's a little different but you should talk to him.

So we flew him to Pittsburgh, we met with him and then we offered him as a job as an analyst and that's how he started, as an analyst in our corporate business and that's what he started with a reporting structure of he reported to an individual by the name of Griffin Schultz who reported to the chief operating officer, Chris Gormley, who then reported to me.¹²¹

* * *

- Q. At what point did Mr. Wallace's work transition from part time for the FBI and full time for the FBI?
- A. **Mr. Wallace was very erratic in his time, so I'm not sure. Sometimes you'd see him; sometimes you wouldn't, in the office.** And he was -- I'm not sure. **It was mostly FBI work. Again, he didn't generate revenue so therefore it was hard for me to say,** I couldn't tie it to revenue coming in so I didn't know, you know, what he was doing.

¹²¹ Boback Tr. at 64-65 (emphasis added).

So he, you know, that's how that went. So, I mean, he was still working as an analyst, obviously, in 2008 and then he, like I said, he was doing both work and then it kind of transitioned out, probably closer to 2009, 2010.¹²²

Expanding on the assertion that Wallace did not generate revenue, Boback told the Committee that Wallace and personally received cash payments from the FBI as a confidential informant, while Tiversa did not receive any money as a result of Wallace's FBI affiliation:

Q. So Mr. Wallace worked with the FBI. It sounds like he was, at times, working in the business-to-government section. Is that fair?

A. But we didn't have any contract with the FBI, so that's why I don't necessarily know where to put him. **He was not a revenue generating** [sic]. In fact, recently it's come to light that Mr. Wallace, it's our understanding that **Mr. Wallace was receiving revenue from the FBI as a confidential informant, yet none of that money ever made it to Tiversa**. So he was keeping that money, that cash that was being given to him, at a reported, as we were told a reported \$1,000 per child pornography case that he gave to the FBI.¹²³

However, a former Tiversa employee told the Committee that Tiversa—or at least Boback—was compensated in cash for Mr. Wallace's work with the FBI:

Q. And do you know whether Tiversa received any compensation from the FBI for Mr. Wallace's work?

A. Yeah. **They were paid cash. I don't know how much. I recall one instance where there was a bag of cash on Molly Trunzo's desk, and it was apparently from the FBI.**

Q. As someone who was responsible, in part, for –

A. About this much. [Estimating the size of the bag].

Q. -- overseeing financial controls at Tiversa, were you concerned that the FBI was paying the company in bags of cash?

A. Yeah.

Q. Did you raise those concerns with anyone at the company?

¹²² *Id.* at 75 (emphasis added).

¹²³ *Id.* at 63 (emphasis added).

- A. This was after my review of Mr. Becker. Yeah, I -- well, I'm trying to remember if I raised those concerns. I definitely raised the concerns during the arbitration hearing, you know, because I wasn't sure whether that was being recorded properly.

The relationship with the FBI itself and how it was set up, I remember Griffin Schultz making a comment and me making a comment at the time as to how we thought it should be handled. And that was another instance of Mr. Boback lashing out at Mr. Schultz. I remember that.

And that was on my -- actually, it was on my comments to Mr. Becker. I remember telling Mr. Becker about any cash and the FBI because I don't know that they were paying us at that time. I think it was just an initial, kind of, trial.¹²⁴

Gormley, the CFO, was apparently not made aware of the cash payments prior to seeing them on Trunzo's desk, and could not say if the money was properly placed in an account.

Later in his transcribed interview, Boback contradicted himself in admitting that Tiversa had received a cash payment from the FBI, although he insisted the money went to Wallace:

- Q. But you don't have any specific information about anything that he downloaded?

- A. He's a confidential informant, and we didn't know. But as I mentioned before, early on Mr. Frankhouser talked to me about knowing that Rick Wallace was on Tiversa's payroll and downloading child pornography presumably for their prosecutions. He discussed paying Tiversa as a confidential informant, of which I think he did. I mean, he may have -- they may have paid us as a confidential informant a little bit. I could double check. I'm not positive. **They may have paid us some money as a confidential informant.**

- Q. So as you understand it, Tiversa is a confidential informant as opposed to Mr. Wallace, personally?

- A. I don't know how the FBI designates it, you would have to look. I know that it ultimately became Mr. Wallace. He said to me, he being Mr. Wallace, said to me, along the way that for work he has been doing with the FBI, he was owed some money, and he was owed so much as a confidential informant. It was like \$1,000, or \$2,000, or something like that.

¹²⁴ Gormley Tr. at 209-210 (emphasis added).

And he said to me, would I mind if he took that as a bonus because he has been doing so much hard work for this. I said, no, I don't mind, meaning put the cash into the account at Tiversa as we always do, record it, because we wanted our revenue to come up, and then we will add the amount to your check with the proper withholdings, and that was the last time, thinking back, that was the last time I ever heard anything talked about money paid as any informant and it's my allegation that he continued to take that money, at a rate of roughly \$1,000 per case, in cash and he took it. So I reported that to the authorities.

Q. I see. And the FBI was paying Tiversa for the information that Mr. Wallace was providing, is that right; there was some kind of contract?

A. No.

[Att'y] No, he didn't say that.

Q. Nothing?

A. Nothing.

Q. I'm sorry if I misunderstood.

A. Yeah, no. It is my allegation that **Mr. Wallace was paid by the FBI as a confidential informant, from monies that should have been directed through Tiversa because he was doing that under our direction and we were paying him a salary to do that**, as I mentioned to you and he decided to take that money himself, which is larceny.¹²⁵

In a separate instance, Boback described Wallace's professional behavior as "normal" before launching into a tangent about how Wallace had a "revenge-based mentality":

Q. How often during the course of his employment at Tiversa, if you could describe it for us, was Mr. Wallace in the office? Was it daily?

A. Yeah. I mean, **he was in there like a normal employee, for the most part. I mean, he would come in and leave just normal.**

Q. Earlier today you mentioned he worked from home a lot and you didn't really know what he was doing.

¹²⁵ Boback Tr. at 120-122 (emphasis added).

A. Well, he worked -- as I testified to, he told us that the best time to catch child pornographers was in the evening. So his working from home was over the night, like at nighttime.

Q. Okay. So –

[Discussion off the record.]

[Att’y] If you could just be clear on that.

A. So he would be in the office and then he would go home and search. I think that Mr. Wallace searched peer-to-peer quite a bit as a part of his normal -- it was almost like his ritual, if you will, for his life, to where he was always searching.

Like he was always in front of a computer screen and always searching something, either online or searching peer-to-peer, whether it was at the office or whether it was at home. He was always –

Q. Did you find that troubling?

A. I work in tech. Everyone's a little bit different. So, I mean, we have -- in tech, you know, you have different personalities. He was no exception of a different personality.

The downside of one of the things that **you recognize is he had a very revenge-based mentality[.]**¹²⁶

However, Boback described Wallace’s duties as much more expansive when the discussion turned to verifying the truth of his testimony before Congress. Boback testified that Wallace was solely responsible for Boback’s testimony before this Committee in 2009. Thus, according to Boback, any blame for inaccuracies in the testimony should fall on Wallace. Boback testified:

Q. Did Tiversa employees identify the source of this information other than France? In other words, France got it from somewhere, so do you know where France got it from? Did Tiversa employees determine that?

A. **You're asking me to testify to what someone else did? I have no idea. I was provided information that I testified to, which I believed to be true and correct, as I just testified to again.**

¹²⁶ *Id.* at 202-03 (emphasis added).

- Q. Yeah, no, no, I hear you. I'm just asking you if you know anything else about the facts underlying.
- A. **I know that Mr. Wallace would have been doing this type of work and provided this information to me, which I then provided, believing it to be true and correct, to Congress.**
- Q. Can you tell us with a little bit more specificity what the information Mr. Wallace provided to you was?
- A. Sure. Again, this was 5 years ago, but **Mr. Wallace would have been responsible for discussing breached files; finding, downloading breached files; locating the location of where those files came from; and then, you know, articulating that to us.** So, you know, producing that information, so therefore any information that I received regarding where a file came from, who was the disclosing source, the file itself all came from him.
- Q. And did he tell you those things?
- A. Yes.
- Q. The source?
- A. Yes.
- Q. The location, the specific location?
- A. Yes.¹²⁷

* * *

- Q. Just to clarify for us, my understanding -- and please correct me if I'm wrong, but my understanding from our earlier conversation was that, you know, **Mr. Wallace was hired, you used the term charity with respect to him working at Tiversa.** I understood that **Mr. Wallace was working primarily on child exploitation or child pornography cases, did a lot of that work from home, and I believe you said you didn't really have a great idea of what he was doing a lot of the time.** So the work that you testified to seems to fall outside the bounds of how you described Mr. Wallace's responsibilities at the company earlier. **Could you help rectify that for us?**

¹²⁷ *Id.* at 107-09 (emphasis added).

- A. **I don't think it needs rectification**, but this -- maybe you misunderstood what we were saying. Mr. Wallace did do child pornography-type work with the FBI, to the best of my knowledge. **Mr. Wallace, as I already testified to, was an analyst at Tiversa, which then would put him in this information.** He also searched for, on his own, in the time when he was searching his child pornography and other things, he would come up with files. **He would download files outside of our system**, because, as I testified, our system was configured to look for a dynamic signature profile which was specific for each client, which does not just take everything. So therefore, Mr. Wallace would come up with random downloads that, again, because he managed to do the search from end to end, we were confined within a very confined space in the confines of our work product.

Mr. Wallace could put whatever search in at any time. Clearly, as I testified to, I wouldn't have searched for U.S. nuclear information. However, Mr. Wallace apparently came up with this U.S. nuclear information, because, again, he could put whatever search in and see the outcome of it. So therefore, when he came to me and said, here, I have this, this is not through the course of our normal work of Fortune 500 clients. So therefore, he was putting whatever search in any time he wanted to then -- I'm assuming, because then he would come up and provide us these files, and then he also detailed where the file was -- where he downloaded it from. **I had no reason to believe it wasn't true, and I testified to that accordingly.**¹²⁸

Boback reverted again to describe Wallace's role as minimal later in the interview. He stated:

- Q. Have you hired anyone to replace Mr. Wallace's work as an analyst for Tiversa?
- A. No, he hasn't been an analyst for years, so he hasn't logged in for a long time.
- Q. I'm just -- I'm confused about this aspect of it, though. I can't get my head around it --
- A. Yeah, okay.
- Q. -- because is he doing work just for the FBI, or is he acting as an analyst? What -- I just -- sorry, I keep asking the same question. I want to understand, though.

¹²⁸ *Id.* at 110-11 (emphasis added).

- A. Yeah, that's okay. He was not -- in my estimation he was not -- **now, granted nobody watched him.** Like on a daily basis, nobody would say, what is every minute of your day happening? So that was out. **But he was not an analyst. He was not sitting in what the analysts do for years.**

* * *

There was never like one job, specifically that, that's all it was. He could be researching how to delete metadata or do something along those lines. He could be researching other cyber crimes. So he was kind of doing this mix hodgepodge of a bunch of different things.

- Q. But he wasn't doing work for Tiversa's other clients?

- A. Correct.¹²⁹

As noted above, multiple current and former employees described Boback and Wallace as exceedingly close, both at and outside of work. To the Committee, however, Boback repeatedly characterized Wallace as a dangerous alcoholic. Boback told the Committee that he was aware of Wallace's poor performance and inappropriate behaviors but failed to terminate him for years, even though Tiversa had terminated numerous other employees during the same time period.

When staff questioned Boback's judgment in continuing to employ Wallace in the face of his purported poor performance and erratic behavior, Boback evaded questions with convoluted tangents about how unwell Wallace seemed or the dangers he allegedly posed. He failed to address his own decision-making, instead highlighting at length Wallace's destructive personality.

F. Tiversa's Unseemly Business Practices

1. Tiversa used fearmongering tactics to generate business

From its inception, Tiversa has marketed itself as a vital tool to be wielded against the "scary" and complex world of the peer-to-peer network. Tiversa largely creates revenue through contracts with companies who desire cybersecurity services. To build their brand and generate clientele, Tiversa uses fearmongering tactics by citing stories of the very most sensitive documents on the peer-to-peer falling into the hands of criminals and terrorists.

Sam Hopkins, the creator of Tiversa's technology, gave the Committee examples of the type of information Tiversa had found on the peer-to-peer network. He stated, "I didn't want to

¹²⁹ *Id.* at 251-52.

see the stuff, so I just stayed out of it all....There's just scary stuff out there."¹³⁰ When asked to explain, Hopkins continued, "Yeah, I mean everyone knows of Snowden. Tiversa has way more than he does and Tiversa has new information on everybody."¹³¹

Hopkins further described files he had seen during the course of his work with Tiversa:

Q. Let's fast-forward to the discussion of the Marine One schematics. You said at one point that the Marine One schematics were, sort of, the least sensitive thing you've seen. Is that fair?

A. I wouldn't say "least." You know --

Q. One of the least.

A. -- a tax return for somebody is probably the least, but definitely not the scariest. **Scariest would be how to fly a 747 sitting in, you know, the hands of an Arab. You know, that was pretty scary.**

Q. And you've seen that on --

A. Oh, yeah.

Q. -- the peer-to-peer networks?

A. Yeah. **Or, you know, some guy collecting tons of explosive information from the military and also how to tow a boat into the harbor in the Pacific, you know. Or one of our -- or all of our bases in the South Pacific, all of their security cameras, exactly where all the gunners are and what the cameras can see and how to gain access, that's pretty scary.**

How to blow up every, you know, big city in America with improvised explosives and exactly what trash cans to stick them in and how to take out bridges, that's pretty scary. Space-based laser stuff, that's pretty scary. Seeing China, Russia, Iran actually grabbing the stuff and seeing it transferred over to them, that was pretty scary.

Q. So who created these documents?

A. Government agencies. Defense contractors.

Q. And these are all in the Tiversa data store?

A. They're out on the peer-to-peer, and Tiversa has some of them.

¹³⁰ Hopkins Tr. at 26 (emphasis added).

¹³¹ Hopkins Tr. at 26 (emphasis added).

Q. But everything you just described, is that in the possession of Tiversa in its data store?

A. **That's where I've seen them, yeah. And, I mean, there's millions of files. I mean, it's everything -- I would not be shocked if everybody's information in this room is sitting out there, from your doctors and accountants and, you know, whatnot. It's out there.**

[Att'y] To be clear, when you say in possession of Tiversa, it's not exclusively in the possession of Tiversa. You got it off the Internet.

A. Yeah, it's peer-to-peer. It's probably still out there, and anyone could go and grab it.

Q. But at the time you viewed this information, it had been downloaded by Tiversa.

A. Yeah.

Q. Were these documents marked "classified," do you know?

A. **Oh, yeah. Tiversa is, and peer-to-peer in general, there's tons and tons of classified.** And Tiversa turned over -- Tiversa was in the strange situation, not so much anymore, of that, you know, **they had droves and droves of classified information on all the wars that were going on over in the Middle East. We could see what was happening every day, with all the stuff that was being leaked.** And the government would come every once in a while and get it, and then, you know, it would just sort of disappear, you know[.]¹³²

Hopkins statements about Tiversa routinely downloading classified information is at odds with what the Committee heard from Tim Hall. Hall told the Committee that much of the information Tiversa provided to him while at NCIS was unclassified.¹³³ Hall also stated that, since he began working for Tiversa, Tiversa had not determined that it was in the possession of a classified document.¹³⁴

Regardless of how often Tiversa actually downloaded classified information, however, their marketing tactics appear to have worked—Tiversa frequently received press regarding its account of the government security leaks. When Hopkins was interviewed by CNET regarding Tiversa's involvement in the Marine One leak, he stressed the wide-ranging nature of inadvertent leaks on the peer-to-peer, even designating it as “the biggest security problem of all time”:

¹³² Hopkins Tr. at 97-99 (emphasis added).

¹³³ Hall Tr. at 39-40.

¹³⁴ Hall Tr. at 35.

- Q. So your team concluded that the materials fell into the hands of Iran. Is it possible that other actors also are trying to take advantage of similar openings in the system?
- A. Heck yeah. Every nation does that. **We see information flying out there to Iran, China, Syria, Qatar--you name it. There's so much out there that sometimes we can't keep up with it.**
- Q. I would have assumed military contractors would use more secure networks to communicate.
- A. Everybody uses (P2P). Everybody. We see classified information leaking all the time. **When the Iraq war got started, we knew what U.S. troops were doing because G.I.'s who wanted to listen to music would install software on secure computers and it got compromised.**
- Q. This is what your company specializes in, obviously, but what's your professional opinion about the extent of this sort of thing?
- A. **This is the biggest security problem of all time.** Coming from me, it sounds biased. But you can get 40,000 Social Security numbers out there at the drop of a hat. **We've had people come into our data center and we've shown them things that are out there on P2P and they go away with their minds blown.**¹³⁵

Various outlets portrayed Tiversa as partnering with federal authorities. One outlet wrote, “By the end of [2004], Tiversa was working with the CIA, FBI, Homeland Security, and the U.S. Secret Service.”¹³⁶ Regarding a WikiLeaks spreadsheet containing potential terrorist targets in California, another outlet wrote, “Asked to aid in the investigation of the leak by U.S. authorities that the company declined to identify, Tiversa found the spreadsheet was inadvertently exposed by a California state employee using a peer-to-peer network in August 2008, more than a year before WikiLeaks posted it.”¹³⁷

Tiversa capitalized on this press in their presentations at various conferences and to potential clients.

2. Tiversa systematically mined for files for “potential” clients as a solicitation tactic.

¹³⁵ Charles Cooper, *Q&A: Tiversa Co-founder Talks About P2P Leak*, CNet (Mar. 1, 2009), available at <http://www.cnet.com/news/q-a-tiversa-co-founder-talks-about-p2p-leak/> (emphasis added).

¹³⁶ John Foley, *Your Data And The P2P Peril*, InformationWeek (Mar. 13, 2008), available at http://www.informationweek.com/your-data-and-the-p2p-peril/d/d-id/1065643?page_number=2. The Committee found many of Tiversa’s claims regarding its relationships with federal agencies to be greatly overstated.

¹³⁷ Michael Rile, *WikiLeaks May Have Exploited Music Networks to Get Data*, Bloomberg (Jan. 20, 2011), available at <http://www.bloomberg.com/news/2011-01-20/wikileaks-may-have-exploited-music-photo-networks-to-get-classified-data.html>.

A whistleblower told the Committee that Tiversa kept dossiers of information on various companies and executives in an attempt to garner new business. According to the whistleblower, Boback even went so far as to create false documents containing large amounts of sensitive information he obtained through his improper use of a law enforcement database to trick potential clients into purchasing Tiversa's services.

As a matter of practice, Tiversa contacted companies whose documents it found on the peer-to-peer network. Tiversa did so under what it called a "duty of care" policy. However, Tiversa held back critical information from companies whose documents were actually exposed in order to force them to purchase Tiversa's services.

When asked whether Tiversa contacted non-client companies about documents actually exposed on the peer-to-peer network, Boback told the Committee that it did not—that Tiversa only searched the data store for potential clients that had a relationship with Tiversa. He then admitted that Tiversa did in fact "cold call" new clients with documents found on the peer-to-peer network, but stated that it was not a "routine practice." He testified:

Q. Can you describe circumstances in which you would mine the data store for a potential client?

A. If the client -- if we know we are -- **if we were contacted or we have some relationship with a certain client and we know we are going to see that client.** Prospective clients, yes, prospective clients and the prospectives, it usually starts with a phone call with a prospective client, as any prospective client would start, you have a phone call with the client. You explain to them about the risks of file sharing, the risks of, you know, what this is, and how information can get out this way.

Most people don't understand it, and they say, can you give me an example, so we go into the data store, not into Eagle Vision. We go into the data store and we usually prepare an example sheet of whatever we have in the data store without looking for it; providing that example --

Q. **Have you ever contacted a potential client after mining the data store for information concerning that potential client?**

A. **I think I -- you lost me there.**

Q. Absolutely. **Have you ever looked in the data store for information, found information, and then contacted a potential client?**

[Att'y] **He can't answer. I'm not sure I'm following you. So company X, we want to get them. Let's look for stuff on company X. We call company X?**

Q. Correct.

[Att’y] Okay, do you follow that?

A. Yes. **No, I don't believe so. We may have, but I don't believe so. It is not a routine practice by any means.**¹³⁸

The Committee found, however, that Tiversa routinely “cold called” clients with documents found on the peer-to-peer network. Under the company’s “duty of care” policy, Tagliaferri regularly called businesses to alert them to exposed documents. In fact, Tagliaferri called companies nearly every day at some points of his employment with Tiversa.¹³⁹ The Committee also spoke with numerous companies that Tiversa contacted seemingly out of the blue about documents it found on the peer-to-peer network. Documents obtained by the Committee further reveal that Tiversa contacted MetLife, NetXert, Open Door, and LabMD regarding use of their services.

¹³⁸ Boback Tr. at 146-47 (emphasis added).

¹³⁹ *Id.* at 132.

From: ifriedman@metlife.com [ifriedman@metlife.com]
 Sent: Sunday, July 27, 2008 4:56:27 PM
 To: hvaletk@metlife.com
 BCC: hvaletk@metlife.com
 Subject: Re: IMPORTANT: MetLife Disability Census Found on Web
 Attachments: graycol.gif; ecblank.gif; doclink.gif; C2030192.gif; C1078101.gif

Harry - nice work. I thought that might be the case.

Harry Valetk

----- Original Message -----

From: Harry Valetk
 Sent: 07/25/2008 05:01 PM EDT
 To: Joseph Carroll
 Co: Ira Friedman; Justin Hixson/Leg/MetLife/US@MetLife; Tom Meenan; Meghan Canty
 Subject: Re: IMPORTANT: MetLife Disability Census Found on Web

“It seems Traversa [sic] solicits business by scanning files online, and bringing them to the company’s attention.”

Hello All,

I found a July 10th article with Traversa cited in it from a separate, but similar incident involving file-sharing networks. It seems Traversa solicits business by scanning files online, and bringing them to the company's attention.

Just a thought.

A Supreme Court justice's birthday and Social Security number were exposed on the Internet after a McLean, Va., investment firm employee used an online file-sharing network at his office.

Supreme Court Justice Stephen Breyer's birthday and Social Security number, and records for about 2,000 other clients of Wagner Resource Group, were stored in the company's private files. The data breach began late last year and ended shortly after a reader of a blog on washingtonpost.com discovered the information in June on LimeWire.

Wagner hired Tiversa to repair the breach.

Tiversa's chief executive said these breaches are common since many employees and contractors install file-sharing software on office computers. LimeWire, like other file-sharing networks, allow computer users to share files directly by linking computers. But Robert Boback said users don't realize such networks may make all files available, not just music or movie files users hope to share.

"This case is unique because of the high profile of the targets. The individuals on this list are at a very high risk, almost imminent, of identity theft," Boback said.

More than a dozen LimeWire members, including some in Sri Lanka and Colombia, downloaded the personal records from Wagner, according to Tiversa officials. The company was alerted after the blog reader told Security Fix blog employees about the breach and the blog contacted Wagner.

Harry A. Valetk
 Corporate Privacy Director
 MetLife Privacy Office
 212.578.2116 (direct)
 Privacy -- Pursue it. Promote it. Protect it. Preserve it.
 Joseph Carroll/Pen/MetLife/US

Joseph Carroll/Pen/MetLife/US
 07/24/2008 03:09 PM

To: Ira Friedman/Leg/MetLife/US@MetLife
 cc: Harry Valetk/Leg/MetLife/US@MetLife, Justin Hixson/Leg/MetLife/US@MetLife,
 Larry Wolff/Leg/MetLife/US@MetLife, Michael Fradkin/Ins/MetLife/US@MetLife,
 Michael Tietz/Ins/MetLife/US@MetLife, Susan

----- Forwarded by Michael Fradkin/metlife.us on 08/02/2008 10:02 PM -----

"Ashish Joshi"
 <A.Joshi@lorandoslaw.com>
 08/02/2008 09:58 PM

To: "Michael Fradkin" <mfradkin@metlife.com>
 cc: "Justin Hixon" <jhixon@metlife.com>, "Larry Wolff" <lwofff@metlife.com>
 Subject: Important - Urgent

Michael:

Thank you for your email. I can talk with you and other MetLife persons on Monday, August 4, 2008. Monday afternoon 4:00 p.m. and 11:00 a.m. EST on Monday, August 4, 2008. Monday afternoon 4:00 p.m. EST for me.

As discussed in our teleconference, a few days ago Netxert received a phone call from an agent of Tiversa, Inc. Tiversa's agent informed Netxert that confidential information containing Netxert's employees' personal information (including but not limited to the employees' social security numbers) has been breached and that this information is available on a "P2P server" on the internet. Tiversa's agent refused to disclose the identity or location of this P2P server that contained the personal information of Netxert's employees. However, Tiversa offered to disclose this information, investigate the source of the breach and take remedial steps *if* Netxert agreed to retain Tiversa's services at \$495/hour. Netxert informed Tiversa that Netxert needed to see a sample of personal information that was allegedly available on the P2P server and then would take the necessary steps. Tiversa emailed Netxert a MS-Excel file that contains personal & confidential information of Netxert's employees including their first and last names, social security numbers, date of birth, gender, marital status, primary details, addresses, etc.

After a preliminary investigation, Netxert has determined that there has been no security breach from Netxert's computer systems and/or servers. The MS-Excel file that was emailed to Netxert by Tiversa contains metadata that shows MetLife as "author" of the file. The Excel spreadsheet states "MetLife Census for Disability" as its heading. The information contained in the spreadsheet was sent to MetLife by Netxert's staff at some point in time in order to obtain disability insurance. At this stage, it appears that MetLife is the source of this security breach.

Frankly, we consider Tiversa's "offer" as nothing short of blackmail. Also, the fact that Tiversa touts itself as MetLife's "vendor" also raises some questions about Tiversa's knowledge and access to this confidential information.

So far, Netxert has not met with the law enforcement authorities to complain about this security breach and Tiversa's tactics. However, soon Netxert will be obligated to (a) inform its employees (residing in several states) and (b) the FBI about this security breach. **Before** we take any of the above steps, we want to meet with MetLife's management and discuss these issues and try and work together to resolve this situation. However, time is of the essence in this matter. **We need to act fast.**

Again, I request you to make MetLife's legal personnel (and other necessary personnel) available for a face-to-face meeting on Monday. If you are not able to get everyone together on this short notice, please try and get your in-house lawyers available for a face-to-face meeting on Monday and the rest can join via teleconference. If not Monday, please schedule a meeting on Tuesday – but it is imperative that we have a face-to-face meeting. I do not want to keep discussing this matter via telephone back and forth.

I await your response. If you have any questions, please feel free to reach me on my cell (734-637-7112) over this weekend.

Thank you.

Ashish

ASHISH S. JOSHI
 LORANDOS & ASSOCIATES
 ATTORNEYS AT LAW
 214 N. FOURTH AVENUE
 ANN ARBOR, MI 48104
 TEL: 734-327-5030
 FAX: 734-327-5032
www.lorandoslaw.com

This e-mail is covered by the Electronic Communications Privacy Act, 18 U.S.C. Section 2510-2521 and is legally privileged. Unauthorized review, use, disclosure or distribution is strictly prohibited. The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and as such is privileged and confidential. If you are not the intended recipient, please contact the sender by reply e-mail, and destroy all copies of the original message. Unintended disclosure does not in any manner whatsoever waive the attorney-client privilege.

From: Michael Fradkin [mailto:mfradkin@metlife.com]

"a few days ago Netxert received a phone call from an agent of Tiversa, Inc."

"Tiversa offered to disclose this information, investigate the source of the breach and take remedial steps *if* Netxert agreed to retain Tiversa's services at \$495/hour"

3. Boback Misrepresented Howard Schmidt's Role in Generating Business Contacts for Tiversa

Tiversa boasts an impressive board of advisors, a corporate governing body separate of the board of directors. The members of the advisory board include Howard Schmidt, General Wesley Clark, Maynard Webb, Larry Ponemon, Michael Dearing, Thomas Keevan, Lynn Reedy, and Patrick Gross.¹⁴⁰ The board purportedly provides “business” and “strategic guidance” to Tiversa.¹⁴¹ Joel Adams praised the involvement of Tiversa’s board. He stated, “Some companies use advisory boards as window dressing...The interaction is minimal, and that type of board isn’t worth much. **Tiversa has been able to get its advisers to interact, to participate. When they walk about of a board meeting, they have to-do lists.**”¹⁴² Contrary to Adams’ praise, however, according to Boback the advisory board met only once, in January 2006.¹⁴³

Instead, Tiversa appears to use the advisory board primarily to solicit clientele. In a bulletin published by Morgan Lewis & Bockius, Boback stated, “when we considered advisers, we asked ourselves, ‘Who can provide instructions? Whose credibility can we leverage to get where we need to be?’”¹⁴⁴ The article goes on to note, “Tiversa added the other [advisors], who became stepping stones to clients... and more.”¹⁴⁵

Howard Schmidt serves on Tiversa’s board of advisors. During his tenure as advisory board member, he was appointed as the White House Cybersecurity Coordinator under President Obama.¹⁴⁶ Upon his appointment, Schmidt put the options he received from Tiversa into a blind trust. When asked by the Committee about Schmidt’s role at Tiversa, Boback expressly denied that Schmidt helped generate business or introduce clients:

Q. Did Mr. Schmidt help generate any business for Tiversa?

A. I don’t believe so.

Q. **Did Mr. Schmidt introduce you or anyone else at Tiversa to potential clients?**

A. **No.**¹⁴⁷

Contrary to Boback’s statement, the Committee has received extensive e-mail correspondence between Boback and Schmidt, where Schmidt systematically introduces Boback

¹⁴⁰ Tiversa Advisory Board, Tiversa, *available at* <http://tiversa.com/about/advisors.html>.

¹⁴¹ Boback Tr. at 28.

¹⁴² Evan Pattak, *Build a Better Board: See How a Solid Board of Directors Can Poise a Company for Success 9*, *Getting It Done II*, *available at* http://www.morganlewis.com/pubs/GettingItDone2BuildABetterBoard_TEQ2007i5.pdf (emphasis added) [hereinafter Pattack].

¹⁴³ Boback Tr. at 29.

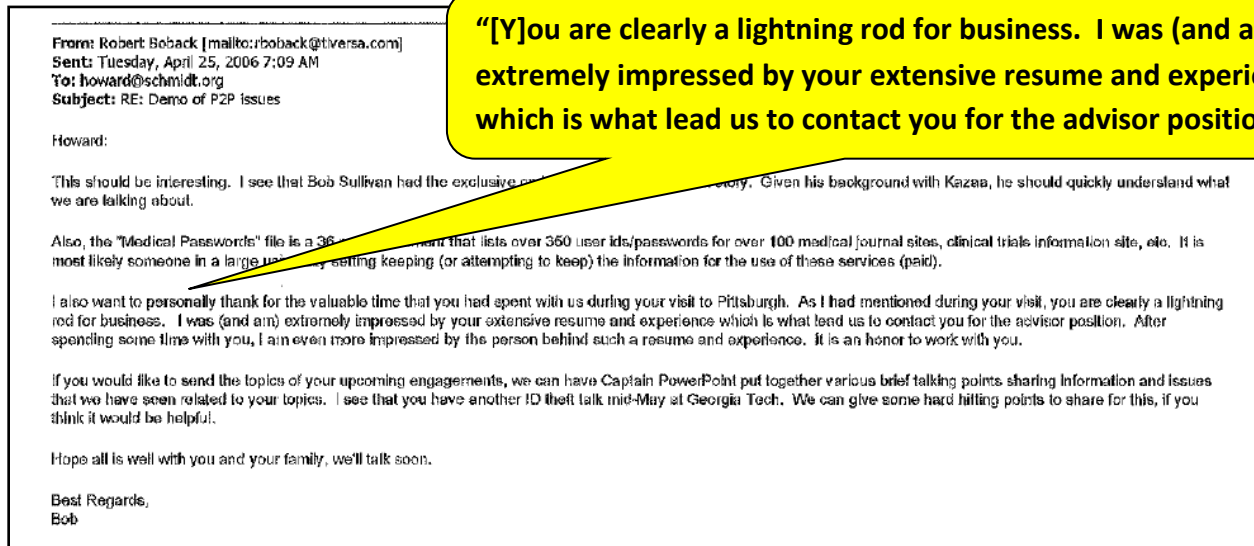
¹⁴⁴ Pattack at 8..

¹⁴⁵ *Id.* (ellipsis in original).

¹⁴⁶ Macon Phillips, *Introducing the New Cybersecurity Coordinator*, *The White House Blog* (Dec. 22, 2009) <http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator>.

¹⁴⁷ Boback Tr. at 41.

to potential clients and media contacts. In one e-mail to Schmidt, Boback praised him as “a lightning rod for business”:¹⁴⁸



Tiversa played in active role in ensuring Schmidt could be an effective advocate. Chris Gormley, copying Boback, gave Schmidt explicit talking points on Tiversa’s business model:¹⁴⁹

¹⁴⁸ TIVERSA-OGR-0017729.

¹⁴⁹ TIVERSA-OGR-0017719.

From: Chris Gormley <IMCEAEX-
_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=CGORMLEY@tiversa.com>
Sent: Monday, May 1, 2006 12:40 AM
To: howard@schmidt.org
Cc: Robert Boback <rbboback@tiversa.com>
Subject: Slides
Attach: Howard043006.ppt

Howard,

Thank you for highlighting the problems we're addressing in your talks over the next 6 days. I've attached some information that may help you on Monday that is focused primarily on the problem in general. I put the files in a neutral file format. The example is a medical one, but it is one that had the least sanitization needed.

What I would like to do is speed time after today (Monday) working up a more helpful set of slides / presentation to support your other talks this week. I envision the slides supporting two sections:

Section 1: Slides showing the problem in general

Section 2: Modules providing examples for:

1. ID Theft
2. Fraud
3. Regulatory Violations

To support Section 2, I have to sanitize some existing examples. Please let me know if other examples will be helpful in section 2. Also, please let me know what I could do to make the slides I sent to you today more helpful including putting slides into templates for your presentations.

Christopher L. Gormley
Chief Operating Officer
Tiversa, Inc.
The Leader in Information Containment Management
Office: 724-940-9030
Fax: 724-940-9033
Mobile: 724-991-3376

This e-mail message and any attachments contain confidential information from Tiversa, Inc. If you are not the intended recipient, you are hereby notified that disclosure, printing, copying, distribution, or the taking of any action in reliance on the contents of this electronic information is strictly prohibited. If you have received this e-mail message in error, please immediately notify the sender by reply message and then delete the electronic message and any attachments.

“Howard, Thank you for highlighting the problems we’re addressing in your talks over the next six days. I’ve attached some information that may help you on Monday...”

Schmidt used these talking points to introduce Boback to potential clients. In June 2006, for example, Schmidt introduced Boback to FAA officials:¹⁵⁰

From: Howard A. Schmidt <howard@cyber-security.us>
Sent: Saturday, June 3, 2006 5:19 PM
To: Michael F Brown <michael.f.brown@faa.gov>; Robert Boback <IMCEAEX-
_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>
Subject: FAA and Data Leakage

Mike,

It was great seeing you at the Arosight meeting and sorry I could not stick around for your presentation.

As I mentioned to you, I have been working with Tiversa and thought that you would find the information that they have found on the P2P networks is unreal. What they have found is not just an errant document here and there but a systemic problem that is found in every sector.

To that end, I would like to introduce you to Bob Boback, the CEO and hopefully you can get a chance to see what they are doing up in Pittsburgh.

Best,
Howard

Sent via BlackBerry - short message and not spell checked.

**“I have been working with Tiversa and thought that you would find the information that they have found on the P2P networks is unreal...
To that end, I would like to introduce you to Bob Boback...”**

¹⁵⁰ TIVERSA-OGR-0017696.

During the same time, Schmidt introduced Boback to Paypal officials, joking that he hoped Paypal would not hold Schmidt's affiliation against Tiversa:¹⁵¹

From: Howard A. Schmidt <howard@cyber-security.tiversa.com>
Sent: Saturday, June 3, 2006 5:10 PM
To: Robert Boback <IMCEAEX-OU=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>; Barrett <nbarrett@paypal.com>
Subject: "Data Leakage" and PayPal

Michael,

I hope this email finds you well and not too swamped. I would like to introduce you to Bob Boback, CEO of Tiversa a company I started working with on some homeland and defense security issues with.

During a recent call I had with Bob we were talking about the widespread issues around data leakage issues with P2P technology (eDonkey, limewire etc.) and he mentioned that there were a number of PayPal related things that his folks had found. I told him that I would let you know.

For full disclosure, I am their advisory board but hopefully you will not hold that against them. :)

Thanks and seeing what they have found, and continue to find, would be worth your time.

Best,
Howard
Sent via BlackBerry - short message and not spell checked.

"I would like to introduce you to Bob Boback... During a recent call I had with Bob we were talking about the widespread issues around data leakage issues... and he mentioned that there were a number of PayPal related things that his folks had found "

"For full disclosure, I am their advisory board but hopefully you will not hold that against them. 😊"

Schmidt also approached Merrill Lynch on behalf of Tiversa, after Boback told him he had unsuccessfully tried to solicit the company:¹⁵²

From: Howard A. Schmidt <howard@schmidt.org>
Sent: Wednesday, April 19, 2006 9:29 AM
To: Robert Boback <IMCEAEX-OU=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>; Basile, Anthony (IS&P) <anthony_basile@ml.com>
Subject: Introduction as we talked about.

Hello Tony and Bob,

It was good talking with both of you recently and I hope this email finds you both well. Tony, as I mentioned I am on the advisory board of Tiversa and during a recent demonstration for some government related documents the discussion came up about data leakage and financial services. What Bob demonstrated for me was not an isolated document that was found but a widespread systemic leakage problem across ALL sectors, energy, telecom, transportation, financial etc. I think you mentioned that you had heard something about Tiversa but this is something that you have to see yourself to believe.

Thanks and I look forward to catching up next time I am in NY.

Best,
Howard

¹⁵¹ TIVERSA-OGR-0017697.

¹⁵² second TIVERSA-OGR-0017740

From: Howard A. Schmidt <howard@schmidt.org>
Sent: Tuesday, April 11, 2006 11:56 PM
To: Robert Boback <[mailto:RBOBACK@tiversa.com]>
Subject: RE: Merrill Lynch

(IN CONFIDENCE) I am working with them taking a look at their security program for their exec team. I will talk with Anthony Basile who has engaged me. Let me know if you want to send some samples.

Thanks
Howard

-----Original Message-----
From: Robert Boback [mailto:RBOBACK@tiversa.com]
Sent: Tuesday, April 11, 2006 3:02 PM
To: howard@schmidt.org
Subject: Re: Merrill Lynch

Hi Howard,
ML is one of the worst when it comes to leakage. We have made initial contact but have been stopped by a mid level IT individual named Swati Dutta Rey. They don't understand the problem. Any assistance that you can lend would be much appreciated.

Thanks
Bob

-----Original Message-----
From: "Howard A. Schmidt" <howard@cyber-security.us>
Subj: Merrill Lynch
Date: Tue Apr 11, 2006 11:44 am
Size: 227 bytes
To: "Robert Boback" <rboack@tiversa.com>

Hi Bob,

I have a consulting job with ML and as I talk with them I wanted to give them some insights into if they were leaking. Have you seen anything?

Thanks
Howard
Sent via BlackBerry - short message and not spell checked.

"(IN CONFIDENCE) I am working with them taking a look at their security program... I will talk with [ML official] who has engaged me."

"We have made initial contact but have been stopped by a mid level IT individual... Any assistance that you can lend would be much appreciated."

Tiversa also leveraged Schmidt's reputation for publicity. Schmidt contacted news outlets on Tiversa's behalf.¹⁵³

From: Howard A. Schmidt [mailto:howard@schmidt.org]
Sent: Monday, April 24, 2006 11:19 PM
To: Robert Boback; Bob Sullivan (MSNBC-JV)
Subject: Demo of P2P Issues

Bob (and Bob, MSNBC) @ ,

Bob Sullivan and I both spoke at an event with the AG for Ohio today on their ID Theft program. After the lunch, I talked with Bob about what you were doing and some of the really dangerous things that you showed me. I also explained to him that you did not want to alienate potential customers and that it would be counter productive to "report" on who had problems (everyone) but it might be a good way for Bob to raise the awareness. He did a story a while back around Kazzaa but I do not think he has seen anything like you showed me.

To that end, I would like to introduce you to each other to see what you can work out. Please let me know if there is anything I can do to help.

Best,
Howard

"I would like to introduce you to each other o see what you can work out."

¹⁵³ TIVERSA-OGR-0017729

The Committee found that, contrary to Boback's statements about Schmidt's role at Tiversa, Schmidt actively sought out contracts and potential clients for the company. This is yet another example of Boback providing false information during the course of this investigation.

4. Boback Misrepresented Information about Tiversa's Capabilities to Clients

According to a former Tiversa employee, Boback had a propensity to exaggerate, or even lie at times. Gormley stated, "the perception at least from what I remember internally was that there was a tendency to exaggerate or at least misrepresent... what was going on at the time."¹⁵⁴ Specifically, the feeling among some employees was that Boback's statements were "60 percent, you know, bullshit; 30 percent not true; and 10 percent truth, I guess, as far as like a representation of the facts."¹⁵⁵

Gormley recalled a specific instance in which Boback misrepresented facts in meeting with a client:

Q. When you say "third parties," do you mean potential clients?

A. I remember the incidents. I mean, one was an existing investor, a limited partner within Adams Capital, came into the meeting, into a discussion, and **the number of employees and the revenues of our companies were overstated at the time.**

The other was, well, to General Wesley Clark and Yahoo around **whether we were profitable or not.** And, again, you know, at the time, we were profitable for one quarter, but we weren't profitable for an entire year. I looked at that as misrepresenting that we're profitable, but you could argue that we were profitable for one quarter.

There were also too many employees attributed to a potential acquirer named SecureWorks. That was later corrected, of course, in diligence, because you know how many employees you have, right?

And those are some of the incidences I remember. And then -- so those are some -- I'm just trying to remember some of the other major areas.

Q. Sir, did you ever confront Mr. Boback about these misrepresentations?

¹⁵⁴ Gormley Tr. at 131-32.

¹⁵⁵ *Id.* at 131, 136.

- A. Yeah, I mean, I told him, you can't do that, they're going to -- particularly in the case of potential acquirers, they're going to find out. I mean, let's not say that. We lose credibility in those instances.

The case of this limited partner, the individual on the other end of the table was someone who friends of mine knew, so I felt personally at odds.

- Q. And this is the gentleman from Adams Capital?

- A. No, it's a limited partner, who was an investor in Adams Capital that came in to see essentially what Adams Capital was investing in. So, I mean, to me, the risks there were lower, because they had already invested. But we can't not state -- now, again, there's all different ways of viewing this. I mean, are you counting every single part-time potential person? Are you counting -- I mean, **but I recall it being an order of magnitude different**; it wasn't close.

So that was one incidence -- set of instances that I remember.¹⁵⁶

In another instance, Boback represented to a potential client that he had a close personal relationship with the FBI, implying retaliatory action if the client did not take action:

[I]n the discussion, Bob mentioned very lightly, but it stood out that he knows people at the local FBI office. And the veiled implication was that continue with monitoring, or else that FBI office might get wind of this.¹⁵⁷

During the course of its investigation, the Committee routinely found that it could not take information provided by Tiversa at face value—and statements made by former employees indicate that clients and potential clients could not do the same. The Committee found that Boback's statements about Tiversa's technological capabilities simply did not match what it found in the documents and testimony, Boback created a hostile work environment, withheld the nature of his relationship with Richard Wallace from the Committee, and created a culture at Tiversa based on a series of unseemly business practices. The Committee found that information provided by Tiversa—such as that on the Marine One leak—not only could not be verified, but at times appeared to be outright false. Given all the Committee has learned about Boback and Tiversa, the extent of its relationship with the Federal Trade Commission is extremely concerning.

V. Tiversa's Relationship with the Federal Trade Commission

¹⁵⁶ *Id.* at 27-29 (emphasis added).

¹⁵⁷ Gormley Tr. at 132-33 (emphasis added).

Tiversa's interactions with the FTC raise questions about the propriety of the relationship. Both Tiversa and the FTC have characterized the relationship as nominal. Overwhelming evidence produced to the Committee, however, demonstrates mutually-beneficial collaboration, wherein the FTC obtained information validated its regulatory authority, and Tiversa gained an ally in a powerful federal agency that provided actionable information that it exploited for monetary gain. Unfortunately, this relationship existed at the expense of good government.

The FTC accepted information from Tiversa through a shell organization without questioning the motives or reason for the third party, or, significantly, the veracity of the underlying information. The FTC's motives for blindly accepting this information are unclear.

In addition, Tiversa's involvement with LabMD, a medical testing laboratory based in Atlanta, Georgia, raises questions. Not only does LabMD's story offer a case study illustrating Tiversa's coercive business practices and relationship with the FTC, but information the Committee obtained shows that Boback lied about material information in the case, which ultimately led to the shuttering of LabMD.

According to a whistleblower, Tiversa withheld from the FTC information about its clients that had data breaches while providing information for companies that rejected the offer to buy Tiversa's services. According to the whistleblower, the FTC blindly trusted Tiversa's data and took only nominal steps to verify the information before embarking on the dissemination of warning letters and enforcement actions. Documents provided by the Federal Trade Commission also indicate the limited steps taken to verify information provided by Tiversa.

A. Tiversa misrepresented the extent of its relationship with the FTC to the Committee

On July 9, 2009, weeks before Tiversa testified before this Committee for the second time, the FTC sent a civil investigative demand to an entity Tiversa created called the Privacy Institute.¹⁵⁸ Tiversa responded promptly, passing documents and information about peer-to-peer breaches at nearly 100 companies through the Privacy Institute, which the Committee learned was created for the sole purpose of funneling information to the FTC pursuant to the CID. When the Committee asked Boback about Tiversa's relationship with the FTC, however, he painted a picture of a government agency bullying a small company. He testified:

We wanted to create separation, as we felt we were being bullied by the FTC into having to provide information to—a small company having to be forced to provide information.

Because in July of 2009, I testified before this committee and then I was bullied by the FTC the very following month, in my opinion, in providing that information.¹⁵⁹

¹⁵⁸ Letter from Reginald Brown, Att'y, Tiversa to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (July 22, 2014).

¹⁵⁹ Boback Tr., at 43 (emphasis added).

Boback reiterated this sentiment by stating:

And we felt -- frankly, as I mentioned, **we felt bullied or trapped to where we were saying I had no choice but to comply with something that was no benefit to Tiversa, was time-consuming, was costly to a small company**, kind of like I feel today.¹⁶⁰

Boback asserted that Tiversa “denied” the FTC’s request for information, and, under threat of a civil investigation demand (CID), Tiversa was compelled to provide information to the FTC.¹⁶¹

Consistent with his stated reluctance to cooperate with the agency, Boback described his contacts with the FTC as very limited. He testified he only knew one person at the FTC—Alain Sheer—and that he only interacted with Sheer on four occasions.¹⁶² According to Boback, Sheer contacted him after the July 2009 Oversight hearing to set up a visit to Tiversa.¹⁶³ A second contact occurred when Sheer visited Tiversa in August 2009. Boback testified about the FTC’s visit to Tiversa:

So he came to Tiversa. They looked in our data center. They went in and said, "We'd like to talk about having" -- we met in our conference room and they said, "We'd like to talk about getting the copies of the information that you provided to House Oversight."

They went into our data center to look at it. And he said, "I want these copy" -- "I need these printed out for us. I need these sent to us." And we said, "We don't send any information from our data center. Our data store is our data store. That is sacrosanct to us. So that's it." And they said, "Well, we're going to need to get this information, and we can use the CID, if necessary." We didn't know what a CID was. He said, "Civil investigative demand, similar to a subpoena. We're going to get the information." And we went, "Oh, no."¹⁶⁴

Yet, by the time this meeting took place in August 2009, Tiversa had already received the CID. It is unclear why the FTC would threaten Tiversa with a CID a month after the CID was issued to the Privacy Institute.

Boback met with Sheer for the third time in Washington, D.C., after the Privacy Institute responded to the FTC’s CID with information it in turn obtained from Tiversa.¹⁶⁵ Then,

¹⁶⁰ *Id.* at 218 (emphasis added).

¹⁶¹ *Id.* at 43.

¹⁶² *Id.* at 188 (Q: “What other attorneys at the FTC, besides Mr. Sheer, have you interacted with?” A: “There were two other attorneys at my deposition in November, but I don’t recall their names... I don’t know anyone at the—the only person I ‘know’ at the FTC is Mr. Sheer.”).

¹⁶³ *Id.* at 184-85.

¹⁶⁴ *Id.* at 185-186.

¹⁶⁵ 186. As discussed below, representatives of the FTC do not recall meeting with Boback in Washington, D.C. It is not clear whether or not this meeting actually took place.

according to Boback, he did not have contact with Sheer until Sheer took his deposition in November 2013.¹⁶⁶ The fourth meeting occurred in June 2014—just before the Committee interviewed Boback.¹⁶⁷

B. The FTC misrepresented the extent of its relationship with Tiversa to the Committee.

The FTC told the Committee that it had limited contact with Tiversa. Representatives from the Division of Privacy and Identity Protection of the Bureau of Consumer Protection told the Committee that the FTC first contacted Tiversa around the time of the July 2009 hearing.¹⁶⁸ FTC officials stated they found Tiversa to be a credible source of information, in large part, because of Boback’s previous testimony before the House Oversight Committee.¹⁶⁹

According to the FTC, after Tiversa sent the information responsive to the CID through the Privacy Institute, all subsequent contacts with Tiversa took the form of clarifying questions about the information provided by Tiversa.¹⁷⁰ Alain Sheer and Kristen Cohen made these calls.¹⁷¹ As described above, FTC officials also recalled a meeting at Tiversa’s offices in 2009, although they could not remember the details.¹⁷² FTC officials did not recall any other meetings with Tiversa. Sheer in particular did not recall meeting with Tiversa in Washington, D.C.¹⁷³

E-mails produced to the Committee—including from entities other than Tiversa—show a much more cooperative relationship between Tiversa and the FTC. Contrary to the assertions Boback made during his transcribed interview as well as those FTC officials made, documents show Tiversa’s relationship with the FTC began in the fall of 2007. In October 2007, Boback participated in a conference call with FTC officials.¹⁷⁴ In December 2007, Boback provided documents to the FTC.¹⁷⁵ In June 2008, FTC attorney Carl Settlemyer thanked Boback for his “cooperation and insights into the area of inadvertent file sharing over P2P networks,” and notified him that “confidential” information Tiversa provided to the FTC related to earlier Committee hearings on P2P networks would be produced to the Oversight Committee.¹⁷⁶ In

¹⁶⁶ *Id.*

¹⁶⁷ *Id.*

¹⁶⁸ Briefing by FTC officials to H. Comm. on Oversight & Gov’t Reform Staff (Sept. 9, 2014) [hereinafter FTC Briefing].

¹⁶⁹ *Id.*

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ *Id.*

¹⁷⁴ E-mail from Robert Boback to Carl Settlemyer, Att’y, Fed. Trade Comm’n (Oct. 22, 2007 3:25 p.m.) [TIVERSA-OGR-0000071]; GoToMeeting Invitation—FTC Meeting 10:30 a.m. to 11:30 a.m.

¹⁷⁵ E-mail from Robert Boback, CEO, Tiversa to Carl Settlemyer, Att’y, Fed. Trade Comm’n (Dec. 19, 2007 3:08 p.m.) [TIVERSA-OGR-0000065]; E-mail from Carl Settlemyer, Att’y, Fed. Trade Comm’n (June 25, 2008 12:13 p.m.) [TIVERSA-OGR-0000063].

¹⁷⁶ E-mail from Carl Settlemyer to Robert Boback (June 25, 2008 12:13 p.m.) [TIVERSA-OGR-0000063] (attached letter from Carl Settlemyer, Att’y, Fed. Trade Comm’n, to Robert Boback (June 25, 2008) [TIVERSA-OGR-0000064]).

March 2009, Boback again participated in a conference call with the FTC.¹⁷⁷ Days later, Boback bragged about the call:¹⁷⁸

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, March 09, 2009 8:59 AM
To: Kline, Eric D.; Todd Davis
Subject: RE: Tiversa comparison

Todd,

I'm in the office today if you want to discuss this after you have had a chance to review. I also wanted to give you an update on the great call that I had with the FTC on ID theft issues.

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

Personnel from the FTC's Division of Privacy and Identity Protection told the Committee that Tiversa's contacts with the FTC prior to the July 2009 hearing took place with a different division of the FTC.¹⁷⁹ Yet, Alain Sheer was included on e-mails with Boback requesting information about a recent Tiversa press release and scheduling the March 5, 2009, conference call¹⁸⁰—the same call that Boback boasted about days later.

Tiversa's phone records are also telling of the company's relationship with the FTC. They indicate that Tiversa employees placed two phone calls to FTC attorney Laura Vandruff in June 2008, and that in the four months leading up to the July 2009 Oversight Committee hearing, Tiversa employees called Alain Sheer at his FTC office on 21 occasions.¹⁸¹ Documents show that Boback was one of the FTC's main contacts at Tiversa prior to July 2009.

Regular phone calls between Tiversa and the FTC took place between August 2009, when Tiversa provided information to the FTC, and January 19, 2010, when the FTC sent letters to nearly all of the companies Tiversa turned over to the FTC. During these months, Tiversa

¹⁷⁷ E-mail from Robert Boback to Carl Settlemeyer, Att'y, Fed. Trade Comm'n (Mar. 4, 2009 1:55 p.m.) [TIVERSA-OGR-0000052].

¹⁷⁸ E-mail from Robert Boback to Todd Davis, CEO of LifeLock, and Eric Kline (Mar. 9, 2009 8:59 a.m.) [LLOCK-OGR-000147]. Tiversa failed to produce this email to the Committee.

¹⁷⁹ FTC Briefing.

¹⁸⁰ See e-mail from Carl Settlemeyer, Att'y, Fed. Trade Comm'n, to Robert Boback, CEO, Tiversa, Stacey Ferguson, Alain Sheer, & Richard Quaresima, Fed. Trade Comm'n (Mar. 4, 2009 5:25 p.m.) [TIVERSA-OGR-0000052-54].

¹⁸¹ Consolidated Comm'ns, Invoice P7249409030020070816TIVERSA_INC [hereinafter Tiversa Phone Records].

employees called Alain Sheer 34 times.¹⁸² The FTC represented to the Committee that only a handful of phone calls ever took place. Tiversa also represented to the Committee that the relationship between Tiversa and the FTC was nominal, and produced few documents indicating any ongoing contract with the FTC after July 2009, let alone this many interactions. The phone records stand in stark contrast to this assessment.

As discussed below, Tiversa used its advanced knowledge of FTC regulatory actions for its own commercial gain.

C. The FTC failed to question Tiversa’s creation of a dubious shell organization, the Privacy Institute, to funnel information to the FTC

Despite the friendly relationship between Tiversa and the FTC, Tiversa asked the FTC to accept documents from a company it created for the sole purpose of responding to the FTC—the Privacy Institute. The certificate of incorporation was filed in Delaware on June 3, 2009.¹⁸³ Boback testified about Tiversa’s purpose in creating the Privacy Institute:

Q. Mr. Boback, what is The Privacy Institute?

A. Privacy Institute is an organization our lawyers set up.

Q. For what purpose?

A. Well, was it originally? I mean, it was –

Q. For what purpose was it set up?

A. Right. It was set up to provide some separation from Tiversa from getting a civil investigative demand at Tiversa, primarily. And, secondarily, it was going to be used as a nonprofit, potentially, but it never did manifest.¹⁸⁴

* * *

¹⁸² *Id.*

¹⁸³ Sec’y of State, State of Del., Div. of Corps., Certificate of Incorporation, No. 4694728 (June 3, 2009) . [hereinafter Certificate of Incorporation]. The Privacy Institute was dissolved on June 18, 2013. On the certificate of dissolution, the address for Brian Tarquinio is that of Boback’s uncle. In a deposition taken just days after the Committee’s transcribed interview, Boback testified that he did not know why his uncle’s address was used on the certificate of dissolution. Deposition of Robert Boback, In the matter of LabMD, No. 9357 (June 7, 2014) at 38. Tarquinio also testified that he did not know why the address of Boback’s uncle was listed as his own on this document. Tarquinio Tr. at 23-24. Upon learning this information, the Committee asked Boback why the address of his uncle was used on this document. Letter from Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov’t Reform, to Robert Boback, CEO, Tiversa (June 23, 2014). One month later, Boback, through his counsel, answered that he did not recall. Letter from Reginald Brown, Att’y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov’t Reform (July 23, 2014).

¹⁸⁴ Boback Tr., at 42.

- A. I don't know if it was their idea or our idea. We wanted to create separation, as we felt we were being bullied by the FTC into having to provide information to -- a small company having to be forced to provide information.

Because in July of 2009, I testified before this committee and then I was bullied by the FTC the very following month, in my opinion, in providing that information.

When we denied providing them information, all of a sudden we were told that, "You have no -- you have no right to deny it, and here's a civil investigative demand that is coming for this."

And we talked to them and said, "We are in acquisition talks at Tiversa and the last thing we want to have is some Federal subpoena or civil investigative demand coming to us."

So our lawyers, in talking to the FTC, they said, "Fine. We'll send this civil investigative demand to this other company, this Privacy Institute, and do it that way."¹⁸⁵

In the same interview, Boback stressed again that the "singular purpose" of the Privacy Institute was to maintain distance between Tiversa and the FTC's CID. Boback stated:

- Q. How would you describe the relationship between the Privacy Institute and Tiversa?

- A. It was one singular purpose that was to make sure or try to do whatever we could so that the FTC did not send a CID, the civil investigative demand, to Tiversa. And that was the only option that our attorneys came up with and the FTC was okay with. So -- or, I don't know if they were okay with it. If they were okay with it, they did it.¹⁸⁶

Boback asked Brian Tarquinio, his financial advisor, to be the President of the Privacy Institute. Tarquinio accepted the request as a "favor" to Boback.¹⁸⁷ Tarquinio had a different understanding of the purpose of the Privacy Institute. Tarquinio stated:

- Q. Could you describe for us what the Privacy Institute is?

- A. I don't think it's anything at this point.

- Q. How about what it was?

¹⁸⁵ *Id.* at 43.

¹⁸⁶ *Id.* at 48.

¹⁸⁷ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Brian Tarquinio (Sept. 5, 2014), at 57 [hereinafter Tarquinio Tr.].

- A. Sure. To my best recollection, **it was an entity that was established to take bids for either part or all of Tiversa if a company wanted to purchase them.**¹⁸⁸

* * *

- A. Sure. My recollection is **it was set up because at the time there were companies that were interested in potentially purchasing Tiversa, and it would be a separate entity to take those bids.**¹⁸⁹

Tarquinio's understanding of the purpose of the Privacy Institute came directly from Boback:

[Att'y] Why don't you just explain how it came to your attention, what your involvement was, and then they'll have follow-ups.

- A. Sure. Mr. Boback came to me and said, we have a company, and at the time I believe it was LifeLock, who was interested in purchasing, you know, some part of Tiversa, which I was aware of. **And he said, we want to create an entity separate from Tiversa to accept those bids, so it is not on our corporate side of everything.** We would like to see if you would be, you know, the head of the Privacy Institute. And as a friend, it seemed pretty reasonable. I said to him, sure, if I get approval [from my employer], fine, glad to.¹⁹⁰

According to Tarquinio, Boback did not inform Tarquinio that the Privacy Institute was set up to transmit information to the FTC. In fact, Boback did not even mention the involvement of the FTC to Tarquinio. Tarquinio stated:

Q. Concurrent with your involvement in the Privacy Institute, were you told that the creation of the Privacy Institute had anything to do with the FTC's interactions with Tiversa?

- A. At that time, no. I had no knowledge of the FTC's interaction with Tiversa.¹⁹¹

Tarquinio had no knowledge that the Privacy Institute had ever transmitted information to any government entity,¹⁹² and only recently learned of the Privacy Institute's connection to the FTC:

¹⁸⁸ *Id.* at 16.

¹⁸⁹ *Id.* at 17.

¹⁹⁰ *Id.* at 20.

¹⁹¹ *Id.* at 21.

¹⁹² *Id.* at 22.

Q. At what point in time did you learn that the Privacy Institute was somehow connected to the FTC? Was it during the course of your preparation for today?

A. Yes, ma'am.¹⁹³

Tarquino's testimony contradicts Boback's explanation of the Privacy Institute's creation, and raises questions regarding the true purpose and activities of the Institute, which remain unknown.

Regardless of the reasons that Boback created the Privacy Institute, it is not in dispute that Tiversa used the Privacy Institute to send information to the FTC. The FTC did not question Tiversa's use of the Privacy Institute, and did not know that the Privacy Institute was set up solely to respond to the FTC's request for information.¹⁹⁴ FTC officials clearly knew that the information was, in fact, coming from Tiversa, despite the use of the Privacy Institute.¹⁹⁵ The FTC admitted that the use of Tiversa's information was unusual relative to standard agency operating procedures for enforcement measures.¹⁹⁶

FTC officials relied heavily on Tiversa's "credible" reputation in "self-verifying" the produced information.¹⁹⁷ The FTC explained to the Committee the steps it took in "self-verifying" the information:

- Tiversa, through the Privacy Institute, certified the information provided under penalty of perjury.
- FTC employees looked up the IP addresses provided by Tiversa to determine if the IP address was affiliated with the company.
- FTC employees looked at the metadata of the documents, when provided, to determine the author or the document.
- FTC employees performed "some" searches on the peer-to-peer networks, both for company names and specific documents. The FTC independently found only one of the files Tiversa submitted on the peer-to-peer network.¹⁹⁸

Ultimately, outside of some minimal work verifying IP addresses and looking at metadata, the FTC relied entirely on the list of companies and documents Tiversa provided. Of the 88 companies Tiversa submitted to the FTC, the agency sent warning letters to 63 companies, and opened investigations into 9 companies.¹⁹⁹ The FTC also issued a press release on the letters

¹⁹³ *Id.* at 22-23.

¹⁹⁴ FTC Briefing.

¹⁹⁵ *Id.*

¹⁹⁶ *Id.*

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

¹⁹⁹ [FTC_PROD16732-16964].

and received considerable media exposure for its new work related to data security. According to the FTC, this was the only time it obtained information from Tiversa.

The FTC further explained that it only needs “reason to believe” that a company is failing to adhere to appropriate data security standards before sending a warning letter or issuing a complaint. The agency was comfortable with the extent of the “self-verifying” steps it took before sending warning letters and opening investigations into nearly 100 companies. The FTC categorically denied to the Committee that it gave Tiversa notice that it would be using the information in letters to companies. Documents the Committee obtained during the course of this investigation suggest otherwise.

D. Tiversa manipulated advanced, non-public, knowledge of FTC regulatory actions for profit

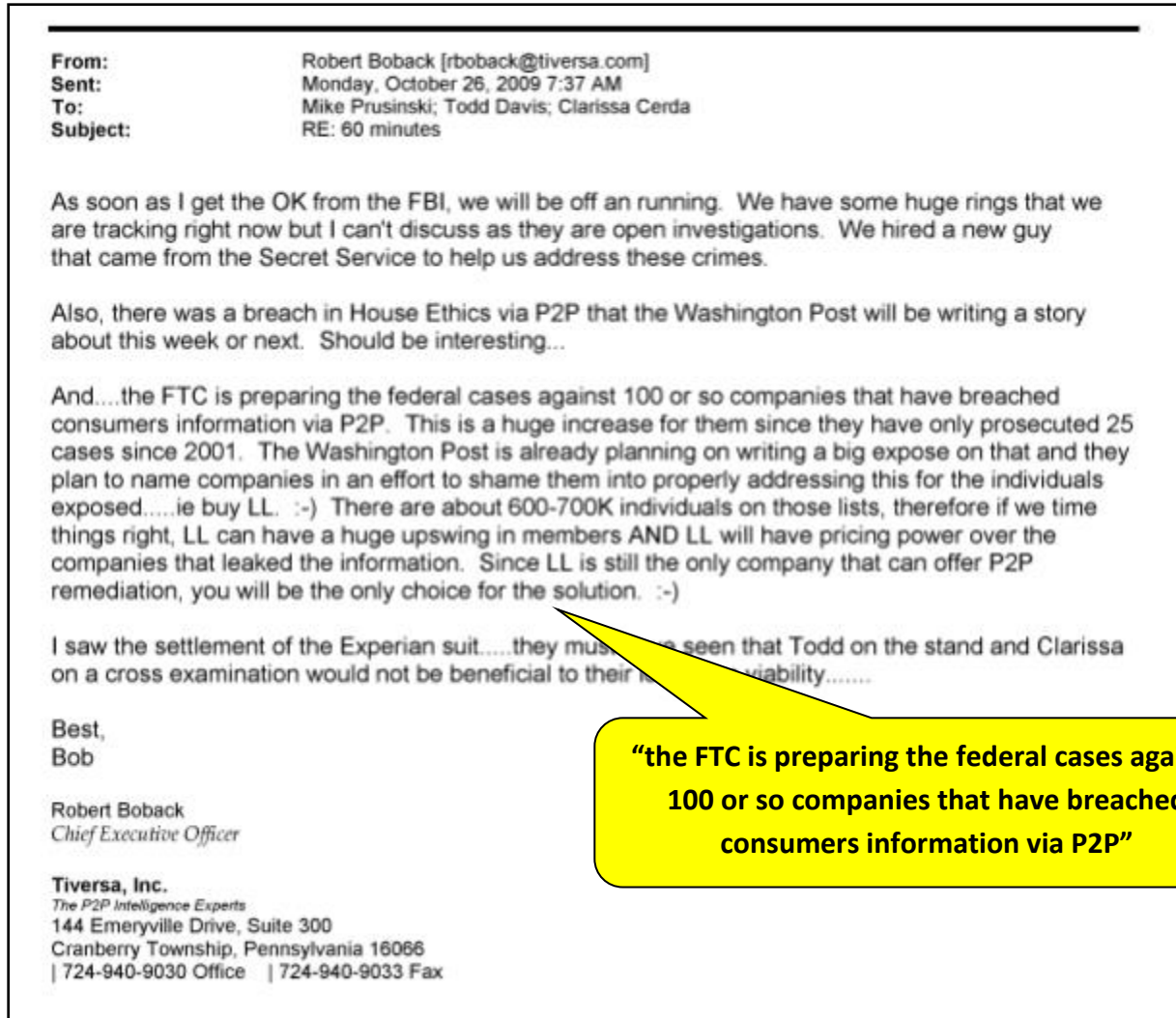
Tiversa had advanced knowledge that the FTC intended to pursue regulatory actions against many of the companies it turned over to the Privacy Institute in response to the CID. FTC officials maintained to the Committee that no one at the FTC provided advance information of the January 2010 regulatory actions to Tiversa.²⁰⁰ Tiversa did not produce the overwhelming majority of the documents indicating Tiversa’s intention to profit off the FTC’s actions. Tiversa failed to produce these documents despite the fact that they were clearly responsive to both the original subpoena, and the search terms provided by Committee staff.²⁰¹ The Committee obtained these documents from other sources.

Armed with non-public knowledge of these impending actions, Tiversa maneuvered to position itself to profit from the FTC’s actions. In the fall of 2009, Boback began working with LifeLock, a major partner of Tiversa and Tiversa’s largest source of income, to send letters to the companies that would be contacted by the FTC—the very companies that Tiversa turned over to the FTC. In October 2009, Boback e-mailed senior LifeLock executives about the impending FTC investigations:²⁰²

²⁰⁰ FTC Briefing..

²⁰¹ Subpoena from H. Comm on Oversight & Gov’t Reform to Tiversa, Inc. (June 3, 2014). The subpoena requires production of “all documents and communications referring or relating to work Tiversa, Inc. performed for the Federal Trade Commission. *Id.* The Committee further provided the search terms “FTC” and “Federal /2 trade /2 commission”.

²⁰² E-mail from Robert Boback to Mike Prusinski, Todd Davis, and Clarissa Cerda (Oct. 26, 2009 7:37 a.m.) [LLOCK-OGR-0002009].



The “100 or so companies that have breached consumers [sic] information via P2P” were the same companies that Tiversa itself reported to the FTC. Boback further explained that the *Washington Post* planned to “shame” companies into addressing the problem, and that the upcoming FTC investigations presented a unique opportunity for LifeLock and Tiversa to profit.²⁰³

Boback’s scheme to profit from the FTC investigations took shape in the coming weeks. In early October 2009, Boback advised LifeLock that “the FTC letters did not go out yet so the companies will not know what you are talking about.....yet.”²⁰⁴ He further advised that LifeLock should “be solo” and “suggest Tiversa if asked by the company.”²⁰⁵

²⁰³ *Id.*

²⁰⁴ E-mail from Robert Boback to Anthony Hesano, LifeLock (Oct. 6, 2009 8:40 a.m.) [LLOCK-OGR-0001929]. Tiversa failed to produce this e-mail to the Committee.

²⁰⁵ *Id.*

----- Original Message -----
From: Robert Boback <rboback@tiversa.com>
To: Anthony Hesano
Sent: Tue Oct 06 08:40:21 2009
Subject: RE: FTC letter

I agree with your approach. The FTC letters did not go out yet so the companies will not know what you will be talking about....yet. I think that it LL should be solo on this.....you could always suggest Tiversa if asked by the company. :-)

It was great to catch up with you and Ally as well. I understand that Jacque is in town this week. Brian is a totally straight up guy that I would absolutely not try anything out of line, or even close to any line.....and I mean that.

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

“The FTC letters did not go out yet so the companies will not know what you will be talking about...yet. I that that... LL should be solo on this... you could always suggest Tiversa if asked by the company. ☺”

The following month, Tiversa and LifeLock’s strategy with respect to the as-yet-unannounced FTC investigations became clear. In a November 3, 2009, e-mail, a LifeLock employee stated that he “spoke with Bob” about repositioning the letter.²⁰⁶ He described the attached version as one that will “get the response we are looking for without overplaying our cards.” Another LifeLock employee responded, stating, “As mentioned, Clarissa has stopped this pending the FTC but our strategy is to send a letter similar to the one outline[d] along with the breach brochure.”²⁰⁷ A later e-mail describes the revised strategy:²⁰⁸

²⁰⁶ E-mail from Gary Woods to Steve McGrady, Eric Warbasse, and Chris Miller (Nov. 3, 2009, 10:35 a.m.) [LLOCK-OGR-0002044].

²⁰⁷ E-mail from Steve McGrady to Gary Woods, Eric Warbasse, Chris Miller, and Austin Colcord (Nov. 3, 2009 12:00 p.m.) [LLOCK-OGR-0002043-2044].

²⁰⁸ E-mail from Gary Woods to Austin Colcord and Chris Miller (Nov. 3, 2009 2:25 p.m.) [LLOCK-OGR-0002043].

From: Gary Woods
Sent: Tuesday, November 03, 2009 2:25 PM
To: Austin Colcord; Chris Miller
Cc: Anthony Hesano; Eric Warbasse; Steve McGrady
Subject: FW: LifeLock Breach Services - intro letter

Austin & Chris

I re-wrote the letter and believe it is on target – and generic enough that Legal is not going to have any issue. I spoke with Eric & Austin about it and now I just need Chris to have Legal approve the verbiage.

Key points:

- No FTC reference
- No Tiversa reference
- No P2P reference

This is solely to make these accounts aware of LifeLock so when they fully realize the need to respond to a data breach – they think of LifeLock first and have our contact information to reach out and partner with us. I’m sure based on discussions with Bob that Tiversa will also be involved with these accounts and will reinforce their need to provide a LL solution in their breach compliance letter to affected individuals.

Thanks for your help,

Gary

“Key points:

- **No FTC reference**
- **No Tiversa reference**
- **No P2P reference”**

As discussed, the draft letter, as provided to Boback on November 3, 2009, contains no reference to the FTC, no reference to Tiversa, and no reference to the peer-to-peer networks.²⁰⁹

On February 22, 2010, the FTC announced that it notified “almost 100 organizations” about data breaches that occurred on peer-to-peer file sharing networks, and opened non-public investigations into several other companies.²¹⁰ Boback sent the link to executives at LifeLock:²¹¹

From: Robert Boback
To: Gary Woods; Todd Davis; Mike Prusinski
Sent: Mon Feb 22 09:30:18 2010
Subject: FTC press release

Guys,

Check out this link.....then ask yourself who knows what's going on?!?!?!?! :-)

<http://www.ftc.gov/opa/2010/02/p2palert.shtm>

Best,
Bob

Robert Boback
Chief Executive Officer

1

²⁰⁹ Draft Letter, LifeLock (undated) [LLOCK-OGR-0002045].

²¹⁰ Press Release, FTC, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), available at <http://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe>

²¹¹ E-mail from Robert Boback to Gary Woods, Todd Davis, and Mike Prusinski (Feb. 22, 2010 9:30 a.m.) [LLOCK-OGR-0002375].

LifeLock responded, “Once again you guys are at the top of the food chain. Any problem with us pushing this with media and using you?”²¹² Boback promptly replied, “No problem.”²¹³

In an interview with *Computerworld* days after the FTC press release, Boback stated, “We were happy to see that the FTC [has] finally started recognizing that P2P is a main source for criminals to gain access to consumer’s personally identifiable information for ID theft and fraud.”²¹⁴ Boback further stated that complying with the FTC’s request for information could be “extensive and cumbersome,” and that 14 of the companies the FTC contacted had already contacted Tiversa for help.²¹⁵ The *Computerworld* article does not mention that Tiversa acted as the primary source for the FTC’s enforcement actions announced in February 2010.²¹⁶

When asked about the propriety of Tiversa seeking to profit from its dealing with the FTC, FTC attorney Alain Sheer stated that it was routine for the FTC to make clear to third parties that the information was not public.

Q. In the course of your interactions with Tiversa in the pre-complaint period, did you or one of your colleagues ever tell Tiversa not to discuss the conversations that the FTC and Tiversa were having with third parties?

A. It is routine for Commission staff to ask entities that are providing information to keep the information confidential.

Q. Do you recall making that specific request to Tiversa? A I don't recall it. Q It would've been your general practice or your colleagues' general practice to make that request? A Yes.²¹⁷

Sheer further testified that he was unaware of Tiversa seeking to profit off of the information provided to the FTC until shown documents produced to the Committee and that the scheme with Lifelock was concerning.

Q. Does it concern you that Mr. Boback seems to have obtained some sort of information about what the FTC planned to do as early as October 26, 2009?

A. The company provided information about roughly 100 companies when they looked at it. They are well aware of what it is they gave to us. So is it a concern?

²¹² E-mail from Mike Prusinski to Robert Boback (Feb. 22, 2010 11:47 a.m.) [LLOCK-OGR-0002375].

²¹³ E-mail from Robert Boback to Mike Prusinski (Feb. 22, 2010 10:00 a.m.) [LLOCK-OGR-0002375].

²¹⁴ Jaikumar Vijayan, *FTC Questions Firms Being Probed for P2P Breaches*, TECHWORLD (Feb. 26, 2010), <http://news.techworld.com/security/3213712/ftc-questions-firms-being-probed-for-p2p-breaches/?olo=rss>

²¹⁵ *Id.*

²¹⁶ Tiversa informed the Committee that it had prior business relationships with 11 companies whose information was included in response to the CID. This conflicts with statements Boback made in the *Computerworld* interview that “14 of the companies contacted over the leaks have already contacted Tiversa for help” and that “all but two of those have CIDs.” Not only is the number of companies with contracts with Tiversa inconsistent, but many of the companies that received CIDs from the FTC did not, in fact, have contracts with Tiversa.

²¹⁷ H. Comm. on Oversight & Gov’t Reform, Transcribed Interview of Alain Sheer, Fed. Trade Comm’n, Transcript at 94 (Oct. 9, 2014) (hereinafter Sheer Tr.).

Yes. I'd like it to be kept confidential. That's the point of asking for it to be kept confidential.²¹⁸

Troublingly, despite Tiversa's close relationship with Lifelock, a company that was itself the subject of an FTC investigation, Sheer stated that he was unaware of the relationship between Lifelock and Tiversa before being informed of it by Committee staff in a transcribed interview.

Q. Are you aware of Tiversa and LifeLock having a -- having a business relationship -- I guess, what is your awareness of Tiversa and LifeLock's business relationship?

A. I don't know that they have a business relationship other than the statement that was made in the -- in the email that you -- that you presented earlier.

Q. Okay. Was the email I presented earlier the first you'd heard of Tiversa and LifeLock having any relationship?

A. Yes.²¹⁹

Boback could not have known the details of the FTC's investigations—including the timing of the letters, which constituted pre-decisional information about pending non-public government actions—without some sort of inside knowledge about the FTC's enforcement plans. While the Committee's investigation has not yet identified the source of the Tiversa's information about the FTC actions, it is clear that Tiversa and the FTC had a mutually beneficial relationship. The FTC used Tiversa as the source of convenient information used to initiate enforcement actions, and Tiversa used the FTC to in further pursuing the company's coercive business practices.

E. Information provided by Tiversa formed the basis of the FTC's case against LabMD

Documents produced to the Committee show that in an effort to generate business, Tiversa repeatedly sought to coerce companies to purchase its services. Tiversa's methods have ranged from contacting a company about a leak but failing to provide anywhere close to full information, to referring nearly 100 companies to the FTC. The Committee has spoken to numerous companies on the list Tiversa provided to the FTC—not one of the companies the Committee contacted had entered into a contract with Tiversa. One such business tangled in Tiversa's web was LabMD.²²⁰ In January 2014, it closed its laboratory operations because of costs incurred by its dealings with Tiversa and the FTC.²²¹

²¹⁸ *Id.* at 107.

²¹⁹ *Id.* at 170.

²²⁰ *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight Gov't Reform*, 113th Cong., at 18 (July 24, 2014) [hereinafter Daugherty Testimony] (statement of Michael Daugherty, CEO of LabMD).

²²¹ *Id.* at 72.

According to Boback, Tiversa downloaded a file containing patients' personally identifiable health information in February 2008.²²² Tiversa determined that the downloaded file likely belonged to LabMD, and contacted the company in May 2008. Tiversa provided LabMD with a copy of the file, but would not provide the IP address or other information unless LabMD agreed to purchase Tiversa's services.²²³

Tiversa referred LabMD to the FTC as one of the companies listed in the spreadsheet as responsive to the FTC's CID. The FTC, in turn, sent a complaint letter to LabMD. The FTC then initiated an administrative enforcement action against LabMD for unfair and deceptive business practices.

Among the information Tiversa gave to the FTC regarding LabMD was the IP address that was the source of the leak. The origin of the IP address from where the LabMD document was pulled was a matter of contention in the litigation between LabMD and Tiversa. On numerous occasions, Boback maintained that Tiversa had pulled the LabMD document from an IP address in San Diego, California:

Q. Going back to CX 21. Is this the initial disclosure source?

A. If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.

Q. When did Tiversa download CX 10?

A. I believe it was in February of 2008.

Q. Has CX 10 changed in any way since Tiversa downloaded it?

A. No.²²⁴

When asked about the Georgia IP address, Boback denied downloading the information from there:

Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?

A. That, if I recall, is an IP address that resolves in Atlanta, Georgia.

* * *

²²² Fed. Trade Comm'n, Deposition of Robert Boback, In the Matter of LabMD, Inc. 25-26 (Nov. 21, 2013) [hereinafter Boback FTC Deposition].

²²³ Daugherty Testimony, at 19.

²²⁴ Boback FTC Deposition, at 25-26.

Q. What other information do you have about 64.190.82.42?

A. I have no other information. I never downloaded the file from them. They only responded to the hash match.²²⁵

In an internal e-mail dated almost three months before the deposition and never produced to the FTC, however, Boback stated that Tiversa downloaded the LabMD file while working for a client. He stated, “The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD’s office to be located. This statement, made by Boback in September 2013, fundamentally calls into question his claim that Tiversa never downloaded the LabMD file from the IP address in Georgia.”²²⁶

From: Robert Boback <rbohack@tiversa.com>
Sent: Thursday, September 5, 2013 3:20 PM
To: Dan Kopchak <dkopchak@tiversa.com>; Molly Trunzo <mtrunzo@tiversa.com>
Subject: Tiversa

I wanted to provide updated information regarding the question of litigation involving Tiversa. During our call, I discussed litigation in which Tiversa is a pla against our former patent firm. That is still ongoing. Earlier in 2013, Tiversa was also engaged in a separate litigation with a company called LabMD, which is base in Georgia. Tiversa, Dartmouth College and Professor Eric Johnson (Tuck Business School) was sued by LabMD by its CEO, Michael Daugherty as he alleged that Tiversa “hacked” his company in an effort to get a file containing nearly 9,000 patient’s SSNs and medical information and provided the information to Dartmouth and Eric Johnson for a DHS-funded research project. Mr. Daugherty has little to no understanding of P2P or Information security which is what caused him to think that he was “hacked” and which resulted in his widespread government conspiracy theory that followed. He also suggested in the litigation that because he would not do business with Tiversa to remediate the problem, that Tiversa “kicked the file over to the feds [FTC]” (and Dartmouth) and the FTC sent him a questionnaire about the breach, which caused him “great harm” due to the widespread “government shakedown of small business.” He claimed that Tiversa was attempting to extort money from him to “answer his questions” as a part of the larger conspiracy. The reason that I did not mention this during our discussion is that the case was dismissed due to jurisdiction (his real estate attorney friend filed it in Georgia). He subsequently appealed two times, and lost both, the final of which was ruled on in February 2013. As an interesting sidebar to this story, Mr. Daugherty began writing a book about the government overreach and his great conspiracy theory o the government war on small business. When our attorneys learned of what was coming in the book (from his blog postings about the book), we quickly served his counsel with a C&D as his “true story” was full of inaccurate statements about me and Tiversa. Unfortunately, Mr. Daugherty sees himself as “Batman” (no joke) and he chose to continue on with his book and starting scheduling speaking engagements where he would discuss his “true story” about how the government is out to “get” small business and that the FTC and Tiversa (and presumably Dartmouth) are the ring leaders. His book, “Devil inside the Beltway” is to be released later this month. While I do not expect this book to be on the NY Times best seller list, I cannot sit idly by and allow such a gross distortion of the facts and mischaracterization of Tiversa, and me, in his efforts to sell his book and create a “name” for himself on any speaking tour.

That said, Tiversa filed a complaint in federal court today citing a number of counts including but not limited to Defamation, Slander, Libel, and others against Mr. Daugherty and LabMD. Tiversa is not litigious and it was our hope that he would conduct himself appropriately after receiving the C&D in November of 2012. But again, he sees himself as Batman.

Here is the real series of events that occurred in this case:

Tiversa, as you know, downloads leaked information on behalf of clients, individual, corporate and/or federal. In the process of downloading information, we often get files that are not related to our clients but are nonetheless sensitive. We call this “dolpin in the tuna net”....for example, if we were looking for “Goldman Sachs” and our system finds a file with the term “Goldman” in it. The file may have the name “Henry Goldman” but our system just saw “Goldman” and downloaded it, in the event it related to Goldman Sachs. After the file would be downloaded, it would be reviewed by an Analyst which would determine that it was NOT related to Goldman Sachs, but it may or may not include SSNs or other sensitive information. This was the case with LabMD.

In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name “LabMD” in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD’s office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable. We could have chosen to do nothing at all and pretend that we never saw the file. That approach would leave both LabMD and the 9000 victims at very high risk (and growing) of fraud and identity theft. Needless to say, we contacted the company to inform them of the file with their company name on it. After providing the file with all of the information that we had, the Mr. Daugherty asked us for additional information that we did not have. We told him that we could perform the services but it would take a few weeks and would cost about \$15K. After hearing this, he asked us to send him the SOW for the services. 3 weeks after providing the SOW and not hearing anything in return, I reached out to Mr. Daugherty to see if he had any questions (re: SOW) and he told me never to contact him again with no further explanation. We did it.

“The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD’s office to be located.”

²²⁵ Boback FTC Deposition, at 41-42.

²²⁶ E-mail from Robert Boback to Dan Kopchak and Molly Trunzo (Sept. 5, 2013 3:20 p.m.) (“The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD’s office to be located.”) [TIVERSA-OGR-0028866].

Further, the initial report that Tiversa provided to a client about the LabMD document stated that the company first “observed” the LabMD file in San Diego, California on August 5, 2008.²²⁷ Tiversa could not have downloaded the LabMD file from an IP address in San Diego in February 2008 if it did not even observe the file at this IP address until August 2008.

In light of the information uncovered by the Committee’s investigation, it appears the FTC was misled as to how Tiversa came to possess LabMD’s file, which has been a material fact in the litigation of the enforcement action. Mr. Sheer testified that, contrary to information provided to the Committee, the FTC had never been told that the file was originally downloaded in Atlanta, Georgia.

Q. Did anyone from Tiversa ever tell you that they first downloaded the file from Atlanta, Georgia, and not from San Diego, California?

A. That wasn't what the testimony was.

Q. Have you seen any documents during the course of your investigation indicating that Tiversa first downloaded the document from Atlanta, Georgia, and not from San Diego, as it testified to the FTC?

A. Not that I am aware of.²²⁸

The discrepancies in the accounts of Tiversa’s downloading of the LabMD file and the information provided to the FTC call into question the FTC’s processes for relying on third-party sources and integrity of its actions against LabMD.

Finally, Tiversa recently performed another forensic analysis on the LabMD file after inexplicably telling the FTC that Tiversa had provided misinformation about the case.²²⁹ This analysis stated that the LabMD file was disclosed by an IP address in Atlanta, Georgia between March 7, 2007, and February 25, 2008.²³⁰ Yet, this information does not comport with the facts of the case. When Tiversa contacted LabMD on [DATE], LabMD performed an investigation and found that a billing manager’s computer had LimeWire P2P software installed, and was sharing the LabMD file. Why did Tiversa’s systems determine that the Georgia IP ceased to share the LabMD file in late February 2008, when LabMD’s own investigation determined that the file was still being shared months later? Why wasn’t this information captured by Tiversa’s technology?

All of this information not only calls into question Tiversa’s technological capabilities, but also Tiversa’s claim that it never downloaded the LabMD file from a Georgia IP address – a

²²⁷ Tiversa Forensic Investigative Report for Ticket #CIG00081 (Aug. 12, 2008) [TIVERSA-OGR-0017461-17465].

²²⁸ Sheer Tr. at 151.

²²⁹ Boback Tr., at 130.

²³⁰ Tiversa Forensic Investigation Report – LABMD0001 (June 4, 2014) [TIVERSA-OGR-0017467-17482].

critical fact in the case against LabMD. As described above, Tiversa's Eagle Vision software purportedly downloads a document every time it hits on a search term. While the software will not download a document from the same IP address twice, it will download the same file from different IP addresses, which indicates the spread of the document. To the Committee's knowledge, Tiversa has not explained in this investigation or other legal proceedings why the software did not download the file from the Georgia IP address. Even assuming that Tiversa was unable to download a file due to technological problems (for example, because the peer-to-peer user signed off while Tiversa was downloading the file), then its software would make another attempt to download the file the next time it was available. Boback has testified that the LabMD file was available on the peer-to-peer network. Either the software does not download a relevant file each time it spreads to a new IP address, which fundamentally calls into question Tiversa's capabilities, or Tiversa did download the LabMD file from the Georgia IP address, a key point in the FTC proceeding.

There is little reason to doubt Boback's statements made to two Tiversa employees—the e-mail clearly shows Boback describing Tiversa's role in the FTC's LabMD enforcement action. Why Boback wrote this e-mail is unknown. It is possible he wanted to make sure he had his facts straight before he was deposed in the FTC matter. Further, Dan Kopchak, to whom Boback sent the e-mail, replied with a draft that made minor edits to the narrative but did not change or question the statement that the IP originated in Georgia.²³¹ Therefore, information the Committee obtained shows that Boback's testimony that source of the IP address came from San Diego is not true. Boback's conflicting statements have broad implications for the future of litigation between LabMD and Tiversa, and calls into question other information he has provided to the FTC.

In short, LabMD witnessed both Tiversa's manipulative business practices and Tiversa's close relationship with the FTC. Evidence produced to the Committee shows that the FTC notified Tiversa of its investigatory schedule, so that Tiversa knew when the Commission would issue complaint letters and act accordingly.

A whistleblower's account of the LabMD saga suggests that the patient data file was only found emanating from a LabMD computer in Atlanta, GA. The whistleblower demonstrated for the committee in tremendous detail how he found IP addresses associated with known identify thieves (also referred to as "information concentrators") and created documents later provided to the FTC showing that the file was in the possession of known-identity thieves when in fact there is no evidence to suggest it was downloaded by anyone other than Tiversa. The reason for forging the IP addresses, according to the whistleblower, was to assist the FTC in showing that P2P networks were responsible for data breaches that resulted in likely harm, not just the exposure of the information from the source computer which could have been easily remedied.

²³¹ E-mail from Dan Kopchak to Robert Boback (Sept. 5, 2013 4:01 p.m.) (revisions from the earlier draft included changes such as "was" to "were;" qualifying "understanding of P2P Information security" to "*may have* caused him to think that he was 'hacked' and which *apparently* has resulted in his widespread government conspiracy theory that followed;" the deletion of "Needless to say," etc.) [TIVERSA-OGR-0025706].

Ultimately, LabMD began to wind down operations in January 2014 as a result of the FTC enforcement action.²³²

F. Tiversa withheld documents from the FTC

The Committee has obtained documents and information indicating Tiversa failed to provide full and complete information about work it performed regarding the inadvertent leak of LabMD data on peer-to-peer computer networks. In fact, it appears that, in responding to an FTC subpoena issued on September 30, 2013, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

1. Despite a broad subpoena request, Tiversa provided only summary information to the FTC about its knowledge of the source and spread of the LabMD file.

Initially, Tiversa, through an entity known as the Privacy Institute, provided the FTC with information about peer-to-peer data leaks at nearly 100 companies, including LabMD.²³³ Tiversa created the Privacy Institute for the specific purpose of providing information to the FTC. Despite Tiversa's claims that it is a trusted government partner, it did not want to disclose that it provided information to the FTC.²³⁴

After the FTC filed a complaint against LabMD, the agency served Tiversa with a subpoena for documents related to the matter. Among other categories of documents, the subpoena requested "all documents related to LabMD."²³⁵ In a transcribed interview, Alain Sheer, an attorney with the FTC's Bureau of Consumer Protection, told the Committee that the FTC did not narrow the subpoena for Tiversa. Sheer stated:

Q. This is the specifications requested of Tiversa. No. 4 requests all documents related to LabMD. Do you know if Tiversa produced all documents related to LabMD?

A. I am not sure what your question is.

Q. Let me ask it a different way. Was the subpoena narrowed in any way for Tiversa?

²³² Michael J. Daugherty, *FTC Actions Force LabMD to Wind Down Operations* (Jan. 28, 2014), <http://michaeljdaugherty.com/2014/01/29/labmd-winds-operations/>.

²³³ Boback Tr. at 42.

²³⁴ See Tiversa, Industry Outlook, Government/Law Enforcement, *available at* <http://tiversa.com/explore/industry/gov> (last visited Nov. 21, 2014); Boback Tr. at 42-43.

²³⁵ Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC Subpoena].

A. Not that I am aware of.²³⁶

In total, Tiversa produced 8,669 pages of documents in response to the FTC's subpoena. Notably, the production contained five copies of the 1,718-page LabMD Insurance Aging file that Tiversa claimed to have found on peer-to-peer networks and only 79 pages of other materials, none of which materially substantiated Tiversa's claims about the discovery of the file.

The information Tiversa gave the FTC included the IP address from which Tiversa CEO Robert Boback has claimed the company first downloaded the LabMD file, as well as other IP addresses that Tiversa claims also downloaded the file. The origin of the IP address from which Tiversa first downloaded the LabMD file was in dispute in other litigation between LabMD and Tiversa. On numerous occasions, including before the FTC, Boback maintained that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. Boback stated:

Q. What is the significance of the IP address, which is 68.107.85.250?

A. That would be the IP address that we downloaded the file from, I believe.

Q. Going back to CX 21. Is this the initial disclosure source?

A. If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.

Q. When did Tiversa download [the LabMD file]?

A. I believe it was in February of 2008.²³⁷

Boback also testified that Tiversa performed an investigation into the LabMD file at the request of a client.²³⁸ In the course of this investigation, Tiversa concluded that an IP address in Atlanta, Georgia, where LabMD was headquartered, was the initial disclosure source of the document. Boback stated:

Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?

A. That, if I recall, is an IP address that resolves to Atlanta, Georgia.

Q. Is that the initial disclosure source?

A. We believe that it is the initial disclosure source, yes.

²³⁶ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer at 147 (Oct. 9, 2014).

²³⁷ In the matter of LabMD, Inc., Deposition of Robert J. Boback, CEO, Tiversa, transcript at 24-25 (Nov. 21, 2013) [hereinafter Boback Nov. 2013 FTC Tr.].

²³⁸ Boback Nov. 2013 FTC Tr. at 72-73 ("In 2008, when working for another client, we were attempting to identify the original disclosure source of the file that we discovered from 1 the San Diego IP address.").

Q. And what is that based on?

A. The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.

* * *

Q. So, I think you are telling me that chronologically this was the first other location for that file in juxtaposition of when you found the file at 68.107.85.250?

A. We know that the file in early February, prior to this February 25 date, was downloaded from the 68.107.85.250. Upon a search to determine other locations of the file across the network, it appears that on 2/25/2008 we had a hash match search at 64.190.82.42, which resolved to Atlanta, which led us to believe that without further investigation, that this is most likely the initial disclosing source.

Q. What other information do you have about 64.190.82.42?

A. I have no other information. I never downloaded the file from them. They only responded to the hash match.²³⁹

Boback's testimony before the FTC in November 2013 made clear that Tiversa first downloaded the LabMD file from an IP address in San Diego, California, in February 2008, that it only identified LabMD as the disclosing source after performing an investigation requested by a client, and that it never downloaded the file from LabMD.

2. Tiversa withheld responsive documents from the FTC, despite the issuance of the September 2013 subpoena. These documents contradict the account Boback provided to the FTC.

On June 3, 2014, the Committee issued a subpoena to Tiversa requesting, among other information, “[a]ll documents and communications referring or relating to LabMD, Inc.”²⁴⁰ This request was very similar to the FTC's request for “all documents related to LabMD.”²⁴¹ Despite nearly identical requests from the FTC and the Committee to Tiversa, Tiversa produced numerous documents to the Committee that it does not appear to have produced to the FTC. Information contained in the documents Tiversa apparently withheld contradicts documents and testimony Tiversa did provide to the FTC.

²³⁹ Boback Nov. 2013 FTC Tr. at 41.

²⁴⁰ H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014).

²⁴¹ Tiversa FTC Subpoena.

An internal Tiversa document entitled “Incident Record Form,” dated April 18, 2008, appears to be the earliest reference to the LabMD file in Tiversa’s production to the Committee.²⁴² This document states that on April 18, 2008, Tiversa detected a file “disclosed by what appears to be a potential provider of services for CIGNA.”²⁴³ The Incident Record described the document as a “single Portable Document Format (PDF) that contain[ed] sensitive data on over 8,300 patients,” and explained that “[a]fter reviewing the IP address, resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.”²⁴⁴ The name of the file was “insuranceaging_6.05.071.pdf,” which is the same name as the file in question in the FTC proceeding. According to the Incident Record, the IP address disclosing the file was 64.190.82.42—later confirmed to be a LabMD IP address.²⁴⁵ Upon learning about the file, CIGNA, a Tiversa client, “asked Tiversa to perform Forensic Investigation activities” on the insurance aging file to determine the extent of proliferation of the file over peer-to-peer networks.²⁴⁶

An August 2008 Forensic Investigation Report provided the analysis CIGNA requested. This report identified IP address 64.190.82.42—the Atlanta IP address—as proliferation point zero, and the “original source” of the Incident Record Form.²⁴⁷ A spread analysis included in the August 2008 forensic report stated that the file had been “observed by Tiversa at additional IP addresses” but made clear that Tiversa had not downloaded the file from either additional source because of “network constraint and/or user behavior.”²⁴⁸ Thus, according to this report, Tiversa had only downloaded the LabMD file from one source in Atlanta, Georgia by August 2008. This contradicts Boback’s testimony that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. If Tiversa had in fact downloaded the LabMD file from a San Diego IP address in February 2008, then that fact should be included in this 2008 forensic report. It is not.

One of the two additional IP addresses is located in San Diego, California. It is a different IP address, however, than the one from which Tiversa claims to have originally downloaded the file.²⁴⁹ Further, Tiversa did not observe that this San Diego IP address possessed the LabMD file until August 5, 2008.²⁵⁰ Thus, according to this report, Tiversa did not observe any San Diego IP address in possession of the LabMD file until August 2008. Again,

²⁴² Tiversa Incident Record Form, ID # CIG00081 (Apr. 18, 2008).

²⁴³ *Id.*

²⁴⁴ *Id.* (emphasis added).

²⁴⁵ *Id.*

²⁴⁶ Tiversa, Forensic Investigation Report for Ticket #CIG00081 (Aug. 12, 2008). This letter uses the phrase “forensic report” to describe this and a second report created by Tiversa about the LabMD file because that is the title used by Tiversa. It is not clear what, if any, forensic capabilities Tiversa possesses.

²⁴⁷ *Id.*

²⁴⁸ *Id.*

²⁴⁹ The IP address reported on the August 2008 forensic report that resolves to San Diego, California is 68.8.250.203. Boback testified, however, that Tiversa first downloaded the LabMD file from IP address 68.107.85.250 on February 5, 2008. Tiversa concluded in the report that the second IP address on which it observed the file was “most likely an IP shift from the original disclosing source.”

²⁵⁰ *Id.*

the report stands in stark contrast to Boback's testimony that Tiversa first downloaded the LabMD file from a different San Diego IP address in February 2008.

In addition, both the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report stated that the LabMD file was "detected being disclosed" in April 2008. Neither report indicated that Tiversa first downloaded the file from the San Diego IP address—an IP address not listed on either report—on February 5, 2008. Boback's deposition testimony and a cursory four-line document marked as exhibit CX-19 seem to be the only evidence that Tiversa first downloaded the LabMD file from a San Diego IP address in February 2008.

These documents contradict the information Tiversa provided to the FTC about the source and spread of the LabMD file. If Tiversa had, in fact, downloaded the LabMD file from the San Diego IP address and not from the Georgia IP address, then these reports should indicate as such. Instead, the San Diego IP address is nowhere to be found, and the Georgia IP address appears as the initial disclosing source on both reports.

Tiversa also produced an e-mail indicating that it originally downloaded the LabMD file from Georgia – and not from San Diego as it has steadfastly maintained to the FTC and this Committee. On September 5, 2013, Boback e-mailed Dan Kopchak and Molly Trunzo, both Tiversa employees, with a detailed summary of Tiversa's involvement with LabMD. Why Boback drafted the e-mail is unclear. He wrote, "[i]n 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."²⁵¹

As noted above, according to Alain Sheer, a senior FTC attorney assigned to the LabMD matter, the FTC did not narrow the September 2013 subpoena requiring Tiversa to produce, among other documents, "all documents related to LabMD."²⁵² Tiversa withheld these relevant documents about its discovery and early forensic analysis of the LabMD file from the FTC. These documents directly contradict testimony that Boback provided to the FTC, and call Tiversa's credibility into question. Boback has not adequately explained why his company withheld documents, and why his testimony is not consistent with reports Tiversa created at the time it discovered the LabMD file.

It is unlikely that the LabMD file analyzed in the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report is different from the so-called "1718 file" at issue in the FTC proceeding, particularly given Boback's testimony to the FTC about how Tiversa's

²⁵¹ E-mail from Robert Boback, CEO, Tiversa, to Dan Kopchak & Molly Trunzo (Sept. 5, 2013) (emphasis added) [TIVERSA-OGR-0028866-67].

²⁵² Tiversa FTC Subpoena.

system names files.²⁵³ If, however, the earlier reports do refer to a different file, then Tiversa neglected to inform the FTC of a second, similarly sized leak of LabMD patient information.

3. Tiversa's June 2014 forensic report is the only report provided to this Committee that substantiates Boback's claims.

Tiversa produced to the Committee a forensic report on the LabMD file that it created in June 2014. Tiversa created this report and others related to testimony previously provided to the Committee after the investigation began. While outside the scope of the FTC's subpoena due to the date of the document, this is the only report supporting Tiversa's claim that it first downloaded the file from the San Diego IP address. This report contradicts information Tiversa provided to CIGNA in the April 2008 Incident Record Form and August 2008 Forensic Investigative Report—documents created much closer to when Tiversa purportedly discovered the LabMD document on a peer-to-peer network. The fact that Tiversa created the only forensic report substantiating its version of events after the Committee began its investigation raises serious questions.

This most recent report states that Tiversa's systems first detected the file on February 5, 2008 from a San Diego IP address (68.107.85.250) not included in either of the 2008 documents. According to the spread analysis, this San Diego IP shared the file from February 5, 2008 until September 20, 2011. Yet, despite allegedly being downloaded before both the April or August 2008 reports, neither 2008 document mentions that Tiversa downloaded this document.

The June 2014 report also states that the LabMD IP address (64.190.82.42) shared the file between March 7, 2007 and February 25, 2008. Thus, according to this report, by the time Tiversa submitted an Incident Record Form to CIGNA in April 2008, the LabMD IP address was no longer sharing the file. Furthermore, the report does not describe why Tiversa's system did not download the file from the Georgia IP address, even though the technology should have downloaded a file that hit on a search term, in this case "CIGNA," each time a different computer shared the document. The June 2014 report includes no reference to the other San Diego IP address discussed in the August 2008 forensic report as being in possession of the LabMD file.

4. Tiversa did not make a full and complete production of documents to this Committee. It is likely that Tiversa withheld additional documents from both this Committee and the FTC.

On October 14, 2014, Tiversa submitted a Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity.²⁵⁴ Chief Administrative Law Judge D. Michael

²⁵³ Boback Nov. 2013 FTC Tr. at 40-41 (describing that a file's "hash" or title identifies "exactly what that file is." The title of the LabMD document described in the April and August 2008 documents is the same as the title of the document in the FTC proceeding).

Chappell has since ordered that the assertions and documents contained in the Notice of Information will be “disregarded and will not be considered for any purpose.”²⁵⁵ Tiversa included two e-mails from 2012 as exhibits to the Notice of Information. According to Tiversa, these e-mails demonstrate that Wallace could not have fabricated the IP addresses in question in October 2013, because he previously included many of them in e-mails to himself and Boback a year prior.²⁵⁶

Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee’s subpoena. Their inclusion in a submission in the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. In its Notice of Information, Tiversa did not explain how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information and do not explain what exactly Wallace conveyed to Boback in November 2012 or why he conveyed it.

If Boback did in fact receive this information in November 2012, his June 2013 deposition testimony is questionable. It is surprising that Tiversa would have supplied inaccurate information to the FTC when Boback himself apparently received different information just months prior. Tiversa should have located and produced these e-mails pursuant to the September 2013 subpoena, and it should have been available for Boback’s June 2013 deposition.

Tiversa’s failure to produce numerous relevant documents to the Commission demonstrates a lack of good faith in the manner in which the company has responded to subpoenas from both the FTC and the Committee. It also calls into question Tiversa’s credibility as a source of information for the FTC. The fact remains that withheld documents contemporaneous with Tiversa’s discovery of the LabMD file directly contradict the testimony and documents Tiversa did provide.

VI. Tiversa’s Involvement with House Ethics Committee Report Leak

A. The Washington Post breaks the story

On October 29, 2009, the *Washington Post* reported that the U.S. House of Representatives Committee on Ethics was investigating the activities of “more than 30

²⁵⁴ Tiversa Holding Corp.’s Notice of Information Pertinent to Richard Edward Wallace’s Request For Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm’n, Oct. 14, 2014), <http://www.ftc.gov/system/files/documents/cases/572572.pdf> [hereinafter Notice of Information].

²⁵⁵ *LabMD Case: FTC gets green light to grant former Tiversa employee immunity in data security case*, PHIprivacy.net, Nov. 19, 2014, <http://www.phiprivacy.net/labmd-case-ftc-gets-green-light-to-grant-former-tiversa-employee-immunity-in-data-security-case/>.

²⁵⁶ Notice of Information at 4.

lawmakers and several aides.”²⁵⁷ The *Post* based its reporting on a “confidential House ethics committee [*sic*] report” inadvertently disclosed on a peer-to-peer network.²⁵⁸ “A source not connected to the congressional investigations” provided the document to the *Washington Post*.²⁵⁹ The Ethics Committee stated that a junior staffer released the document after installing peer-to-peer software on a home computer.²⁶⁰ The staffer was subsequently fired.²⁶¹

The *Washington Post*’s story indicated that the leaked “Committee on Standards Weekly Summary Report” provided summaries of non-public ethics investigations of nineteen lawmakers and several staff members, as well as non-public investigations into fourteen additional lawmakers undertaken by the Office of Congressional Ethics.²⁶²

The same day that the *Washington Post* published its story, Chairwoman Zoe Lofgren made a brief statement about the leak on the House floor.²⁶³ News of the leak prompted a review of the House’s information systems to determine whether there had been any breach beyond the inadvertent leak of the Ethics Committee document on the peer-to-peer network.

Tiversa began providing written information about the leak to the House Ethics Committee in early November 2009, after the *Washington Post* broke the story. Documents produced by Tiversa, however, show that Boback was aware of the leak and its significance more than a week before the story was published. On October 20, 2009, a Tiversa analyst e-mailed Boback the name, resume, and Facebook profile picture of a House Ethics Committee staffer.²⁶⁴ The subject line of the e-mail read, “US Rep Ethics Doc Leaker.”²⁶⁵ On October 26, 2009, four days before the *Washington Post* published its story, Boback wrote an e-mail to executives at LifeLock. He stated:²⁶⁶

²⁵⁷ Ellen Nakashima & Paul Kane, *Dozens in Congress Under Ethics Inquiry*, WASH. POST (Oct. 30, 2009), available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/10/29/AR2009102904597.html>.

²⁵⁸ *Id.*

²⁵⁹ *Id.* In a subsequent *Washington Post* online question and answer forum, the Post further described that the Ethics Committee document was brought to its attention by “a source familiar with those kinds of [peer-to-peer] networks.” *Washington Post Q&A with Carol Leonning 1* (Oct. 30, 2009), available at http://www.washingtonpost.com/wp-dyn/content/liveonline/discuss/transcript_politics131.htm (last visited Sept. 4, 2014).

²⁶⁰ Nakashima.

²⁶¹ *Id.*

²⁶² *Id.*

²⁶³ Chairwoman Lofgren stated, “I regret to report that there was a cyberhacking incident of a confidential document of the committee. A number of Members have been contacted by The Washington Post, which is in possession of a document. We don’t know with certainty whether it is an accurate document, but we thought it important to state the relevance of the material.” Statement of Congresswoman Zoe Lofgren, Cong. Record, Announcement by the Chairwoman of the Comm. on Standards of Official Conduct (Oct. 29, 2009).

²⁶⁴ E-mail from Rick Wallace, Analyst, Tiversa, to Robert Boback, CEO, Tiversa (Oct. 20, 2009 12:34 a.m.) [TIVERSA-OGR-0026603 - 26604].

²⁶⁵ *Id.*

²⁶⁶ E-mail from Robert Boback, CEO, Tiversa, to Mike Prusinski, Vice President, Pub. Affairs, LifeLock, Todd Davis, CEO, LifeLock, and Clarrisa Cerda, Counsel, LifeLock (Oct. 26, 2009 7:37 a.m.) [LLOCK-OGR-0002009].

<p>From: Robert Boback [rboback@tiversa.com] Sent: Monday, October 26, 2009 7:37 AM To: Mike Prusinski; Todd Davis; Clarissa Cerda Subject: RE: 60 minutes</p>	<p>“...there was a breach in House Ethics via P2P that the Washington Post will be writing a story about this week or next...”</p>
---	---

As soon as I get the OK from the FBI, we will be off an running. We have the huge rings that we are tracking right now but I can't discuss as they are open investigations. We hired a new guy that came from the Secret Service to help us address these crimes.

Also, there was a breach in House Ethics via P2P that the Washington Post will be writing a story about this week or next. Should be interesting...

Boback did not explain to LifeLock how he had become aware of the breach, or of the upcoming, and then-unpublished, *Washington Post* story.

While it is suspicious that Boback knew of the *Washington Post* story days before its publication, this Committee’s investigation did not examine whether Boback or Tiversa acted as the initial source in providing the Ethics Committee document to the *Washington Post*. Documents produced by Tiversa showed that Boback provided information about the leak to the *Washington Post* reporter. On October 30, 2009, at 4:49 p.m., a *Washington Post* reporter e-mailed Boback asking whether a certain statement, including a quote from Boback, was accurate:²⁶⁷

<p>From: Ellen Nakashima <nakashimae@washpost.com> Sent: Friday, October 30, 2009 4:49 PM To: Robert Boback <rboback@tiversa.com> Subject: RE: this accurate?</p>
--

A confidential House Ethics Committee file that disclosed the status of dozens of investigations of lawmakers on issues ranging from influence lobbying to defense peddling is still available on public file-sharing computer networks, according to a security firm that specializes in scouring such networks for clients. The document, a committee report from late July, has been downloaded by a handful of users in Washington DC, Houston, New York, Los Angeles, Toronto and London, said Robert Boback, chief executive of Tiversa Inc., the firm that was able to confirm the document was still on the networks yesterday and has technology capable of allowing it to see what tens of millions of computer users are searching for or downloading in real time on these publicly accessible networks. The file was disclosed inadvertently by a junior staffer on the ethics committee, who apparently had stored the file on a home computer that had on it popular “peer-to-peer” software used for downloading free music and movies through file-sharing networks, Congressional sources said. The staffer could not be reached for comment. Her father said her attorney had advised that she not speak about the case. The peer-to-peer premise is simple, and potentially risky. Anyone who has the software makes contents of their computer available to anyone else with the software on their computer through a “peer to peer” exchange bypassing the Web, as long as they are on a file-sharing network at the same time. The staffer, who was the Committee’s Web administrator and developed electronic spreadsheets and documents, was fired earlier this week, the sources said.

.....

Tiversa did not produce to the Committee any response Boback may have written. This is the earliest document produced to this Committee indicating that the document had “spread,” i.e., that other peer-to-peer users had downloaded it. The *Washington Post* does not appear to have used Boback’s quote or the information about the spread of the document in stories about the leak.

²⁶⁷ E-mail from Ellen Nakashima, Wash. Post, to Robert Boback, CEO, Tiversa (Oct. 30, 2009 4:49 p.m.) [TIVERSA-OGR-0026594].

The reporter then e-mailed Boback regarding the origin of the leak. The first sentence reiterated the known information about the leaker, and the second sentence outlined generally how peer-to-peer networks operate:

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 7:47 PM
To: Robert Boback <rboack@tiversa.com>
Subject: RE: this accurate?

In the breach, the report was disclosed inadvertently by a junior staffer on the ethics committee, who apparently had stored the file on a home computer that had so-called "peer-to-peer" software, congressional sources said. The popular software, which is easily available online, allows computer users to share music or other files. But it also allows anyone with the software on their computer to access documents of another user without permission, as long as the users are on a file-sharing network at the same time.

Ellen Nakashima
The Washington Post
202 334 4419 direct
202 286 0552 cell

<http://projects.washingtonpost.com/staff/articles/ellen-nakashima/>

Again, Tiversa did not produce any response from Boback. The e-mail does further illustrate, though, that the reporter sought advice from Boback, at the very least, during the drafting of an upcoming piece.

Several hours later, the same reporter e-mailed Boback a third time with additional information about the leak, including "the latest" on the response by House leaders:²⁶⁸

²⁶⁸ E-mail from Ellen Nakashima to Robert Boback (Oct. 30, 2009 8:08 p.m.) [TIVERSA-OGR-0026592].

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 8:08 PM
To: Robert Boback <rboback@tiversa.com>
Subject: amended

File sharing networks are made up of hundreds of millions of users who periodically log on and off, with 25 million or so being active at any given moment. The typical user, when searching for files, will reach only a small portion of the users on the network--from 30 to 3,000 people, depending on the connection strength. A search on the word "meeting" may result in anything from a PTA meeting to an Iraqi operations meeting involving sensitive military details.

Here's the latest :

House leaders on Friday called for an "immediate and comprehensive assessment" of congressional cybersecurity policies, a day after an embarrassing data breach that led to the disclosure of details of confidential ethics investigations.

Speaker Nancy Pelosi (D-Calif.) and Minority Leader John A. Boehner (R-Ohio) said they had asked the chief administrative officer of the House to report back to them on the policies and procedures for handling sensitive data as a result of the breach. The breach led to the inadvertent disclosure of a House Ethics Committee document that summarized the status of investigations into lawmakers' activities on subjects ranging from influence peddling to defense lobbying.

"We are working diligently to provide the highest level of data security for the House in order to ensure that the operations of House offices are secure from unauthorized access," Pelosi and Boehner said in a statement.

The breach angered lawmakers who were the subject of previously undisclosed investigations and raised questions about the security of other sensitive documents. Rep. Gary Miller (R-Calif.), who was named in the document as having his real estate dealings under investigation, said he was so upset about the breach that he complained Thursday evening about the matter to Rep. Zoe Lofgren (D-Calif.), chairman of the ethics committee, during a series of roll-call votes.

"This is ridiculous and amateurish," he said of the breach in the committee's files.

Even as the House leadership sought answers — and the Ethics Committee moved to review its own security policies — the newly disclosed document remained available on public file-sharing computer networks, according to security experts. As of Friday, it had been downloaded by users in Washington, New York, London and elsewhere.

Ellen Nakashima
 The Washington Post
 202 334 4419 direct
 202 286 0552 cell

<http://projects.washingtonpost.com/staff/articles/ellen+nakashima/>

Again, Tiversa did not produce any response to this e-mail Boback may have written. It is therefore unclear if Boback did not respond at all to these three e-mails, responded by phone, or responded in e-mails that Tiversa failed to produce. In the third e-mail, however, information on the spread and availability is no longer attributed to Tiversa. Instead, it is attributed to "security experts." It is thus not clear if Boback asked that Tiversa not be named in the story, or if the reporter amended the information to exclude Tiversa's name without prompting. Two months later, in December 2009, Boback provided the same reporter with information about a TSA document Tiversa found on the peer-to-peer network. In that instance, Boback wrote, "[a]s always, we are not the source. :-).]"²⁶⁹ The reporter responded, asking "[w]hat again is the main reason you don't want to be identified as the source – to avoid charge [sic] that you're doing this for commercial gain? To preserve relationship with govt [sic] customers?"²⁷⁰

²⁶⁹ E-mail from Robert Boback to Ellen Nakashima (Dec. 17, 2009 2:12 p.m.) [TIVERSA-OGR-0008473].

²⁷⁰ E-mail from Ellen Nakashima to Robert Boback (Jan. 4, 2010 10:36 a.m.) [TIVERSA-OGR-0008473]. Even this exchange runs contrary to statements Boback made to a potential client in July 2008. At that time, Boback wrote about another Washington Post reporter, "I know that the WashPost reporter is actively scouring the file sharing networks to find any information relevant to 'DC-area businesses...especially government contractors.' For clarity, we would never provide any information or files to any reporter whether you decided to work with our firm or not, however he will probably find them on his own if he continues to search." E-mail from Robert Boback, CEO, Tiversa, to [Redacted Name], President/CEO [Redacted Company] (July 17, 2008 2:55 p.m.) (Emphasis and ellipsis in original) [TIVERSA-OGR-0019195]. Given that Boback did, in fact, provide information to a reporter on at least one occasion, it is not clear if Boback lied to this customer about Tiversa's relationship with the media, or if Boback changed his mind about this policy sometime later.

Tiversa did not produce any response to this e-mail from Boback. As such, his reasoning remains unknown.

Less than a year later, in August 2011, Tiversa entered into a contract with TSA for peer-to-peer monitoring and remediation services. The potential value of the contract over five years was \$1,548,000 and the scope of the project included “help[ing] the TSA avoid negative publicity and exposure through P2P file sharing networks.”²⁷¹ TSA did not exercise all option years on the contract. The Committee does not know how many years of the contract passed before TSA ended its contract with Tiversa.

Tiversa received a great deal of press attention in the wake of the House Ethics leak. *Network World* reported that Tiversa had “seen the file at multiple locations including London, Toronto, Washington, Los Angeles, Texas and New York.”²⁷² The leak also sparked additional media interest around Tiversa’s previously announced peer-to-peer discoveries.²⁷³ In one instance, a blogger reported that Tiversa discovered the document.²⁷⁴ Boback insisted that Tiversa deny “discover[y]” of the exposed report to a blogger; he maintained that Tiversa only “investigated” the breach after he was made aware of its occurrence.²⁷⁵ As of September 12, 2014, the article remained unedited.²⁷⁶

Whether or not Tiversa “discovered” the leak, the documents show that although Tiversa was aware of the leak, the company failed to report the leak to the House Ethics Committee, long before the *Washington Post* reported about it.

B. Tiversa “assists” the House Ethics Committee in its investigation

While Tiversa was aware of the Ethics Committee leak more than a week before it became public, Tiversa does not appear to have contacted the Ethics Committee about the leak

²⁷¹ Contract HSTS03-11-C-CIO554 (Aug. 3, 2011) [TIV-0000101-135].

²⁷² Jaikumar Vijayan, *Leaked House Ethics Document Spreads on the Net via P2P*, NETWORK WORLD (Oct. 30, 2009), available at <http://www.networkworld.com/article/2252989/securityeaked-house-ethics-document-spreads-on-the/security/leaked-house-ethics-document-spreads-on-the-net-via-p2p.html> (originally published in *Computerworld*) (last visited Sept. 9, 2014).

²⁷³ J. Nicholas Hoover, *Bill Would Ban P2P Use by Federal Employees*, INFORMATIONWEEK (Nov. 18, 2009), available at <http://www.informationweek.com/regulations/bill-would-ban-p2p-use-by-federal-employees/d/d-id/1084955> (last visited Sept. 9, 2014) (“In October, Tiversa provided the House Oversight and Government Reform committee [*sic*] with evidence that secret military documents on P2P networks had been downloaded in China and Pakistan and that personally identifiable information on U.S. soldiers was widely available.”).

²⁷⁴ John Pescatore, *The Security Risks of Consumerization Hit Home for US Congress*, GARNER BLOG NETWORK (Nov. 2, 2009), http://blogs.gartner.com/john_pescatore/2009/11/02/the-security-risks-of-consumerization-hit-home-for-us-congress/ (last visited Sept. 12, 2014).

²⁷⁵ E-mail from Robert Boback, CEO, Tiversa, to Scott Harrer, Brand Dir., Tiversa (Nov. 11, 2009 10:54 a.m.) (In response to an article by John Pescatore that read “I live in the Washington DC area and much Beltway buzz about the Washington Post article on Tiversa’s discovery of a House ethics report only available on a peer to peer music stealing file sharing network,” Boback said, “Tiversa did not discover the document.... we need to let Pescatore know about that. We only investigated the breach.”) [TIVERSA-OGR-0026558].

²⁷⁶ Pescatore..

prior to publication of the story by the *Washington Post*. Tiversa appears to have first spoken with the House Ethics Committee on or around November 2, 2009.

On November 2, 2009, Boback provided information about the leak to the House Ethics Committee. Specifically, Boback provided a list of IP addresses at which the House Ethics Committee document had allegedly been downloaded.²⁷⁷

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Monday, November 02, 2009 10:13 AM
To: Stoddard, Clifford
Subject: File Spread Analysis (Tiversa)
Importance: High
Sensitivity: Confidential

Mr. Stoddard,

Please see (below) the preliminary file spread analysis that Tiversa performed. Per our discussion, I have instructed our Security Ops Team to issue takedown notices for all of the cases listed. We will continue to monitor to verify that a) no other instances of spread arise and b) the takedown notices are effective in removing the file from the PCs and therefore the network. The IP address in red below is the original source of the leak.

216.45.59.122	UNITED STATES	CALIFORNIA	LOS ANGELES	OC3 NETWORKS & WEB SOLUTIONS LLC
70.240.108.51	UNITED STATES	TEXAS	HOUSTON	AT&T INTERNET SERVICES SWBELL.NET
69.119.255.103	UNITED STATES	NEW YORK	YONKERS	OPTIMUM ONLINE (CABLEVISION SYSTEMS)
72.225.253.212	UNITED STATES	NEW YORK	NEW YORK	ROAD RUNNER HOLDCO LLC
99.234.251.73	CANADA	ONTARIO	TORONTO	ROGERS CABLE INC.
81.76.50.206	UNITED KINGDOM	ENGLAND	LONDON	ENERGIS UK
69.255.116.72	UNITED STATES	DISTRICT OF COLUMBIA	WASHINGTON	COMCAST CABLE
98.218.86.107	UNITED STATES	VIRGINIA	ALEXANDRIA	COMCAST CABLE
76.111.69.89	UNITED STATES	VIRGINIA	ARLINGTON	COMCAST CABLE
68.48.69.117	UNITED STATES	DISTRICT OF COLUMBIA	WASHINGTON	COMCAST CABLE

If you have any questions, please email or call.

Best Regards,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The 22P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16006
| 724-940-9030 Office | 724-940-6033 Fax

The locations of the IPs—including Washington, D.C., Houston, New York, Los Angeles, Toronto, and London—were the same as those included in the e-mails from the *Washington Post* reporter to Boback several days earlier. In a later e-mail that same day, Tiversa provided additional information about when it first located the Ethics Committee document.²⁷⁸

²⁷⁷ E-mail from Robert Boback, CEO, Tiversa, to Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm. (Nov. 2, 2009 10:13 a.m.) [TIVERSA-OGR-0002413].

²⁷⁸ E-mail from Robert Boback to Clifford Stoddard (Nov. 2, 2009 4:44 p.m.) [TIVERSA-OGR-0002412].

“As an answer to your question below, the search that resulted in us finding the original source file occurred in early August. It is my assumption that it was the same day in which the source of the leak saved it to her home PC. The file, although downloaded in early August, was not reviewed by anyone here at Tiversa until recently (2 weeks ago).”

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Monday, November 02, 2009 4:44 PM
To: Stoddard, Clifford
Subject: RE: File Spread Analysis (Tiversa)
Sensitivity: Confidential

Hi Cliff,

Our systems first acquired the file in early August using the term "report." As we provide services for ID theft protection through our partner LifeLock, we issue several general search terms for information related to consumer security such as personal, financial, meeting, password, login, medical, insurance, etc. The results of these, and our other client specific search terms, are downloaded to our storage arrays. We have algorithms and individuals who then review the data via specific criteria (either specific consumer names, SSNs, DOBs, etc. or specific client names like Goldman Sachs, Cigna, Capital One etc.) to determine if our clients information has been exposed. Our searches and downloads happen continuously and downloads have averaged in excess of 100,000 new files per day. As an answer to your question below, the search that resulted in us finding the original source file occurred in early August. It is my assumption it was the same day in which the source of the leak saved it to her home PC. The file, although downloaded in early August, was not reviewed by anyone here at Tiversa until recently (2 weeks ago). I am not sure if I had spoken to Oversight about this specific file as we were discussing several files at that time. Our system can also download additional files (in an automated fashion) from the same source IP in an effort to provide our CFAs (Cyber Forensic Analysts) with additional insight as to the identity of the source of the disclosure. In this situation, our system downloaded two resumes from one of the IP addresses. It was due to the resume that we were able to arrive at a suspected original source.

Unfortunately, there is no way to tell exactly when the secondary IP addresses downloaded the file.

We will continue to monitor for the presence of the file on the network as others may have downloaded the file in addition to the IPs provided. Once detected, we will issue takedown notices with the corresponding ISPs.

Best Regards,
 Bob

Robert Boback
 Chief Executive Officer

Tiversa, Inc.
 The P2P Intelligence Experts
 144 Emeryville Drive, Suite 300
 Cranberry Township, Pennsylvania 16066
 | 724-940-9030 Office | 724-940-9033 Fax

Before Boback sent any e-mails to the House Ethics Committee on November 2, he e-mailed a LifeLock executive about the leak as an “FYI,” in case LifeLock “want[ed] to piggyback anything on this[.]”²⁷⁹

²⁷⁹ E-mail from Robert Boback, CEO, Tiversa, to Mike Prusinski, Vice President, Pub. Affairs, LifeLock (Nov. 2, 2009 9:50 a.m.) [LLOCK-OGR-0002036].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, November 02, 2009 9:50 AM
To: Mike Prusinski
Subject: File sharing breach in House Ethics
Attachments: 20091029183511871.pdf

Pru,

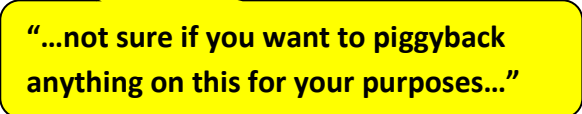
Not sure if you saw the latest file sharing breach in Congress. See attached letter that Congress released regarding the breach. Congress is now doing a complete cybersecurity review and analysis. :-)

Just an FYI for you guys....not sure if you want to piggyback anything on this for your purposes....

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax



Several days later, Boback traveled to Washington, D.C. to meet with the Chair and Ranking Member of the House Ethics Committee regarding the leak.²⁸⁰ During this meeting, the Ethics Committee appears to have requested a timeline from Tiversa about the leak.²⁸¹ On November 24, the Ethics Committee again requested a timeline, apparently after additional phone conversations between the Committee and Tiversa.²⁸² On December 3, the Ethics Committee requested yet again that Tiversa provide the timeline first requested nearly a month earlier. The Ethics Committee also asked if Tiversa’s systems had picked up the file’s download from Wikisecrets.org and several other websites:²⁸³

²⁸⁰ E-mail from Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm., to Robert Boback, CEO, Tiversa (Nov. 6, 2009 2:30 p.m.) [TIVERSA-OGR-0002411].

²⁸¹ E-mail from Blake Chisam, Staff Dir. & Chief Counsel, Comm. on Standards of Official Conduct, to Robert Boback, CEO, Tiversa (Nov. 24, 2009 2:43 p.m.) (“I know Cliff’s been chatting with you about the timeline that the Chair and Ranking Member discussed with you at our meeting ... I can’t recall seeing a timeline. Is there any chance you could shoot that over to me?”) [TIVERSA-OGR-0002409]. Tiversa has not produced any documents to this Committee indicating that it replied to this request for information.

²⁸² *Id.*

²⁸³ E-mail from Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm., to Robert Boback, CEO, Tiversa (Dec. 3, 2009 7:20 a.m.) [TIVERSA-OGR-0002407].

On Dec 3, 2009, at 7:20 AM, "Stoddard, Clifford" <Clifford.Stoddard@mail.house.gov> wrote:

Bob,

Sorry to pester you but in turn I am being asked continually about the time-line issue. I understand that Tiversa system discovered the document on August 4. The global search was done on October 30. Between then, you notified the Oversight Committee, specifically, Steven Rangel. Did you find out the specific date you notified Rangel? Also, as you probably know, the document has now been made available by Wikisecrets.org and can be downloaded from several websites. Did your system pick up these new addresses?

Also, could you have someone send us the hash for the file? Thanks.

The Members will be meeting with us in an hour and will ask again for the timeline I am sure.

Regards,

Cliff

Clifford C. Stoddard, Jr.

Counsel

Committee on Standards of Official Conduct

U. S. House of Representatives

HT-2, the Capitol

Washington DC 20515

(202) 226-8810 (direct)

Boback finally responded, with a very general timeline of events:²⁸⁴

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Thursday, December 03, 2009 10:32 AM
To: Stoddard, Clifford
Subject: Re: information

Hi Cliff

I am in LA training with FBI LEEDA right now but I wanted to drop you a note in advance of your meeting. Our systems located the file on Aug 1 not Aug 4. We did perform a global scan on Oct 30. I spoke to Steven Rangel between those dates but I don't have any record of it to provide clarity as to when. During that period I probably had 15 or so conversations with him regarding other breaches. To the best of my recollection, I think that I spoke to him about the document around the week of 19th of Oct, although it may have been sooner. We only discussed it once. Beyond that, I don't specifically recall anything. It didn't seem that sensitive to me.

Best
Bob

Sent from my iPhone

Boback did not address the Ethics Committee's concern that the file had been made available by wikisecrets.org and several other websites. Boback also provided information that contradicted his November 2, 2009, e-mail. On November 2, Boback wrote that he "was not sure if [he] had spoken to Oversight about this specific file as we were discussing several files at that time."²⁸⁵ On December 3, 2009, however, Boback wrote that he spoke with an Oversight Committee staffer sometime between August 1 and October 30, likely around October 19.²⁸⁶

²⁸⁴ E-mail from Robert Boback to Clifford Stoddard (Dec. 3, 2009 10:32 a.m.) [hereinafter Boback-Stoddard Dec. 3 E-mail] [TIVERSA-OGR-0002407].

²⁸⁵ E-mail from Robert Boback to Clifford Stoddard (Nov. 2, 2009 4:44 p.m.) [TIVERSA-OGR-0002412].

²⁸⁶ Boback-Stoddard Dec. 3 E-mail..

Boback further explained that he “probably had 15 or so conversations” with the Oversight staffer about other breaches between August 1 and October 30, and that he only discussed the Ethics file with the Oversight staffer on one occasion. Boback explained that the file “didn’t seem that sensitive” to him.²⁸⁷

Further, Boback indicated in the November 2 e-mail that Tiversa reviewed the House Ethics document “about two weeks ago,” meaning that Tiversa became aware of the House Ethics file in mid-October. This timeline fits with an October 19 conversation with the Oversight staffer, and the October 20 internal Tiversa e-mail in which Boback received information about a House Ethics staffer.

Tiversa, by its own admission, learned of the House Ethics document in mid-October. Boback had a conversation about the document with the House Oversight Committee, mentioned the leak to executives at LifeLock, and conducted an investigation into the source of the leak, all before publication of the story. Yet Tiversa does not appear to have contacted the House Ethics Committee about the leak prior to publication of the *Washington Post* story. Boback further appears to have provided information about the spread of the leak to the *Washington Post* days before he provided the same information to the Ethics Committee.

Had Tiversa notified the Ethics Committee about the leak in a timely fashion, then it could have prevented some or all of the alleged spread of the document over the peer-to-peer network. When presented with a chance to minimize harm to the House of Representatives, Boback failed to act. Instead, Boback’s failure to inform the House Ethics Committee of the leak quickly and his failure to provide timely and consistent information about the exposed document are indicative of Tiversa’s questionable business practices in general. Finally, Tiversa stood to benefit from the *Washington Post*’s publication of the House Ethics leak regardless of whether Tiversa was the initial source of the article, or whether the article cited Tiversa. Any news on the vulnerability of sensitive information to leaks breached via peer-to-peer networks—and especially a high-profile breach—would bolster Tiversa’s profile as a firm with the capability to remediate this type of problem. The House Ethics leak is another example of Tiversa’s use of its association with Congress as a platform for intimidation and fearmongering.

A whistleblower’s account of the story states that in the course browsing the P2P network for profitable material, Tiversa came across the Ethics Committee document. Tiversa’s plan, according to the whistleblower was to leak the document to the press and generate publicity for it and then sell its services to the U.S. congress as the solution to the problem while never acknowledging it was the source of the breach. This resulted needlessly in the embarrassment of many Members of Congress who did not receive investigatory due process as a result of the pending investigations being exposed.

VII. *Open Door Clinic*

²⁸⁷ *Id.*

The Open Door Clinic is a small non-profit healthcare organization located in Elgin, Illinois.²⁸⁸ Open Door provides education, testing, and treatment for sexually transmitted infections, including HIV/AIDS.²⁸⁹ Between 2008 and 2009, Tiversa sought to exploit the Open Door Clinic using information Tiversa discovered on a peer-to-peer network.

A. Initial contact with Tiversa

On June 5, 2008, a computer with the IP address of 75.58.87.97 disclosed six files related to the Open Door Clinic on a peer-to-peer network.²⁹⁰ According to information provided by Tiversa, through the Privacy Institute, to the FTC, Tiversa appears to have downloaded these six files from that IP address on or around June 5, 2008.²⁹¹ The documents—spreadsheets of patient information—exposed the names, addresses, telephone numbers, social security numbers, and HIV/AIDS status of approximately 250 Open Door patients.²⁹² The fact that patient information was leaked on a peer-to-peer network is not disputed, nor is the seriousness of the leak in question. The documents contain no information identifying them as the property of the Open Door Clinic—the clinic’s name does not appear on any or the six spreadsheets, nor does its address, phone number, location, or any identifying information appear.²⁹³ Tiversa has not provided information to the Committee about how it determined that these documents belonged to the Open Door Clinic.

On July 14, 2008, a Tiversa sales representative contacted the Open Door Clinic about the leak.²⁹⁴ Tiversa subsequently provided one of the six documents it downloaded to the Open Door Clinic via e-mail.²⁹⁵ In the e-mail, which included the password to open the document, the

²⁸⁸ *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight & Gov’t Reform*, 113th Cong. 25 (July 24, 2014) (testimony of David Roesler, Exec. Dir. of Open Door Clinic) [hereinafter Roesler Testimony].

²⁸⁹ Open Door Clinic, *History*, available at <http://www.opendoorclinic.org/about-us/history/> (last visited Sept. 4, 2014).

²⁹⁰ Microsoft Excel spreadsheet from Tiversa to FTC, “FTC Final 8-14-09pm.xls” [FTC_PROD0000014].

²⁹¹ *Id.* The exact date of download of all six documents is not fully clear to the Committee. The spreadsheet of companies created by Tiversa for the FTC indicates that the “date of disclosure” of the six Open Door Clinic files was June 5, 2008. *Id.* Tiversa informed the Committee, however, that it downloaded one of the files, “Master List.xls,” on May 26, 2008 at 7:29 p.m. Letter from Reginald J. Brown, Counsel for Tiversa, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov’t Reform (Aug. 28, 2014). Tiversa declined to provide the exact dates it downloaded the additional five files related to the Open Door Clinic “because Tiversa, Inc. believes it only analyzed the origins of the MASTER LIST.xls file.” *Id.* It is not clear how Tiversa determined the date of disclosure of the six files provided to the FTC to be June 5, 2008, and why Tiversa did not inform the FTC that at least one of the files provided was downloaded the previous month. It is also not clear how Tiversa provided a “date of disclosure” to the FTC for all six documents if it in fact only analyzed one of the files.

²⁹² Microsoft Excel spreadsheet from Tiversa to FTC, “Master List.xls” [FTC_PROD0005345].

²⁹³ Microsoft Excel spreadsheets from Tiversa to FTC, “Master List January 15, 2003.xls” [FTC_PROD0005340]; “Master List Michelle.xls” [FTC_PROD0005341]; “Master List Rosa.xls” [FTC_PROD0005342]; “Master List Sally.xls” [FTC_PROD0005343]; “Master List Sharon.xls” [FTC_PROD0005344]; “Master List.xls” [FTC_PROD0005345].

²⁹⁴ E-mail from Perry Maier, Assistant Dir., Open Door, to Anders Riedemann, IT Adm’r, Adnet (July 14, 2008 10:56 a.m.).

²⁹⁵ E-mail from Keith Tagliaferri, Cyber Forensic Analyst, Tiversa, to Anders Riedemann, IT Adm’r, Adnet (July 14, 2008 3:20 p.m.).

sales representative attached a statement of work for the Open Door Clinic to hire Tiversa.²⁹⁶ The quoted rate for Tiversa’s services was \$475 per hour – far beyond the clinic’s modest budget.²⁹⁷ Open Door employees were immediately suspicious as to why Tiversa contacted the clinic:²⁹⁸

Perry Maier

From: Perry Maier [perrym@opendoorclinic.org]
Sent: Monday, July 14, 2008 2:15 PM
To: Anders Riedemann
Subject: Phone call

Importance: High

Anders: I hope that you will have a chance to speak with Katey. It could be an elaborate scheme to get business. Keep me posted. I believe she gave you her cell phone number. Perry

“It could be an elaborate scheme to get business.”

The Open Door Clinic began an internal investigation of the leak after receiving notification from Tiversa. In early September 2008, an IT vendor for the clinic contacted Tiversa by telephone to obtain more information about the leak and what steps the clinic could take to remediate the breach.²⁹⁹ Tiversa provided eight steps that Open Door could undertake to remediate the leak:³⁰⁰

²⁹⁶ E-mail from Katy Everett to Anders Riedemann, IT Adm’r, Adnet (July 14, 2008 3:29 p.m.) [Open Door e-mail #5].

²⁹⁷ Roesler Testimony, at 25.

²⁹⁸ E-mail from Perry Maier to Anders Riedemann (July 14, 2008 2:15 p.m.).

²⁹⁹ E-mail from Katy Everett, Tiversa, to TJ Vinz, Adnet (Sept. 4, 2008 1:34 p.m.).

³⁰⁰ *Id.*

Tuesday, January 26, 2010 1:26 PM

Subject: P2P Disclosure Information
Date: Thursday, September 4, 2008 1:34 PM
From: Katy Everett <keverett@tiversa.com>
To: TJ Vinz <tvinz@adnet.us>

Hi TJ. Thank you for taking the time to speak with me on the phone this afternoon. What follows is some information you can share with the folks at Open Door in terms of recommendations we would make or best practices we have seen others follow when facing similar circumstances regarding a potential breach. First, please know that though this type of incident is not a new problem, the exposure of it as an issue is new. Extremely large companies with very sophisticated IT systems have been victim to sensitive and costly P2P disclosures (such as Pfizer, ABN AMRO, Walter Reed Army Medical Hospital, etc.) and few if any organizations are immune to its risk.

When a disclosure like this occurs, companies often go through the following steps:

1. Identify the offending computer/source (it may or may not be the computer that you have identified)
2. Identify any additional files that might have been disclosed from the offending computer/source (this often determines/confirms the original source because often additional files are disclosed that allow us to profile the individual disclosing them)
3. Remediate/close down the offending computer/source
4. Identify any additional sources that may have acquired the file(s) and are re-sharing it/them to the P2P networks
5. Remediate/close down any additional sources found in step #4
6. Take any notification steps required by state/industry regulatory bodies based on the severity of the information disclosed (e.g. social security numbers, etc.)
7. Provide services (e.g. credit monitoring, fraud alerts, etc.) to affected individuals
8. Document all steps taken to address both this incident and to prevent others from occurring as required by state/regulatory bodies, customers, other stakeholders, etc., and in support of any future legal defense actions

As I said earlier, Tiversa can assist Open Door with any of the above and in performing the global spread analysis we discussed. This helps many organizations inform their security breach notification proceedings as it will tell you how far the file has spread and how many pcs currently have downloaded it. As we discussed, even though the file itself may appear old, social security numbers never expire and criminals hunt for them every day on these networks in an effort to commit identity theft or fraud against individuals.

Tiversa also offered to “assist Open Door with any of the above and in performing the global spread analysis we discussed.”³⁰¹ The sales representative again attached a statement of work for an Incident Response Investigation for Open Door. The quoted rate remained \$475 per hour.³⁰²

One hour later, the Open Door Clinic’s IT vendor sent these eight steps to the clinic, as well as information on how the clinic had already addressed each step in the course of its internal investigation.³⁰³ The clinic’s internal investigation, based on the limited information provided by

³⁰¹ *Id.*

³⁰² *Id.*

³⁰³ E-mail from TJ Vinz, Adnet to Ryan Howater, Adnet (Sept. 4, 2008 2:40 p.m.).

Tiversa, found that none of the computers on the system had peer-to-peer software installed, and that no peer-to-peer network ports into or out of the clinic's computer system were allowed.³⁰⁴ As Executive Director David Roesler testified, the clinic was at a loss as to how the one file Tiversa provided could have been exposed on a peer-to-peer network.³⁰⁵

Later that month, Tiversa again contacted the Open Door Clinic, this time attempting to sell LifeLock's identity theft services.³⁰⁶ A Tiversa sales representative wrote, "Tiversa has recently established an exciting new partnership with a company called LifeLock. LifeLock is a leading provider of identity theft PREVENTION [*sic*] services to many organizations and corporations."³⁰⁷

Ultimately, Open Door declined to purchase Tiversa and LifeLock's services. In his testimony before the Committee, Roesler explained that the clinic did not purchase Tiversa's services because Open Door's IT provider had sufficiently "reviewed its network to confirm that there was no evidence of any P2P software."³⁰⁸

B. Tiversa only provided self-serving information to the Open Door Clinic in July 2008

Tiversa has maintained to the Committee that it went above and beyond in trying to help the Open Door Clinic mitigate the peer-to-peer leak. Such a statement, however, is not only self-serving, but also incorrect. In fact, Tiversa failed to provide full and complete information about the leak to the clinic.

Several of the eight steps for mitigation Tiversa suggested to the clinic—including the suggestions to "identify any additional sources that may have acquired the file(s) and are re-sharing them to the P2P networks" and "remediate/close down any additional sources found in step #4"—are steps that seemingly require the use of Tiversa's technology. Tiversa has maintained that it provides technology and services that no other company can provide. The so-called "steps" Tiversa provided are in fact a blatant sales pitch. Tiversa failed to provide additional files downloaded from the Open Door Clinic on the same day from the same IP address. Tiversa also failed to provide the IP address of the computer leaking the files, information that Tiversa's technology can provide in minutes. Had Tiversa chosen to provide the Open Door Clinic with this information, the clinic could have more readily identified the source of the leak.

Further, Tiversa appears to have begun investigating the source of the Open Door leak even prior to July 14, 2008, when it first contacted the Open Door Clinic. On July 3, 2008, Chris

³⁰⁴ *Id.*

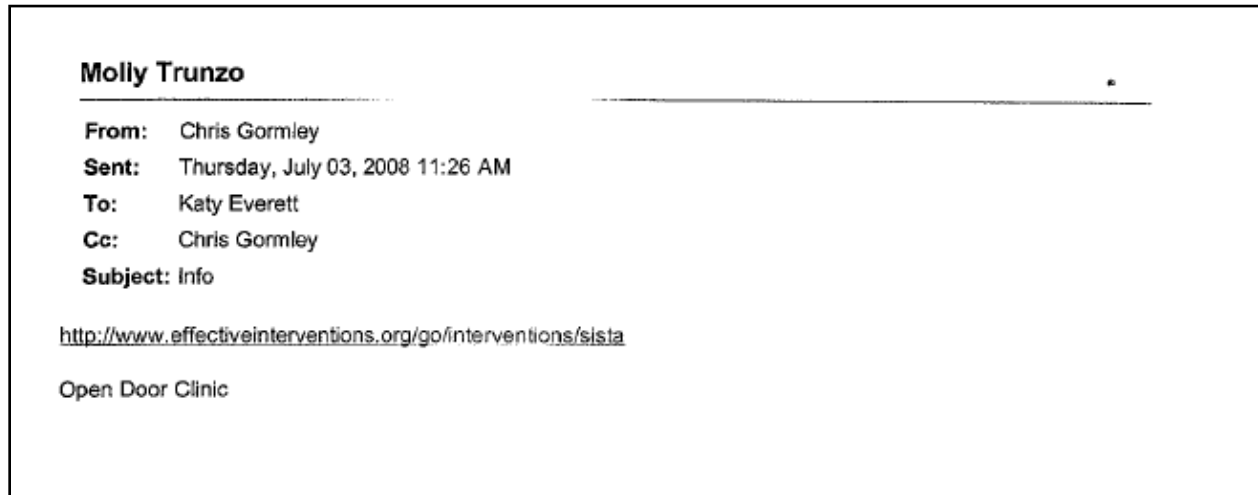
³⁰⁵ Roesler Testimony, at 25.

³⁰⁶ E-mail from Katy Everett, Tiversa, to TJ Vinz, Adnet (Sept. 24, 2008 2:20 p.m.). This e-mail was not produced to the Committee by Tiversa.

³⁰⁷ *Id.*

³⁰⁸ Roesler Testimony, at 25, 60.

Gormley, Tiversa's former Chief Operations Officer, e-mailed a sales representative a web link, with the notation "Open Door Clinic:"³⁰⁹



Tiversa did not produce this e-mail to the Committee. A forensic report Tiversa created in October 2011, which Tiversa also did not produce to the Committee, includes several files about the "SISTA Project" to support its conclusion that the probable disclosure source was a specific Open Door employee.³¹⁰

The July 3, 2008, e-mail indicates that Tiversa had already begun work on step one of the eight steps provided to the Open Door Clinic—"identify the offending computer/source"—but failed to inform Open Door of this information. Further, the same sales representative who sent the eight steps to the Open Door Clinic also received Gormley's e-mail.

Had Tiversa really wanted to help this non-profit clinic, it could have provided all of the files downloaded from Open Door and the IP address of the computer sharing the files in question. Tiversa could have also informed the clinic that it had already begun investigating the source of the breach, and had identified a potential link between documents the computer shared and the identity of the computer's owner.

C. Tiversa facilitates a class action lawsuit against the Open Door Clinic, and contacts Open Door patients directly

On July 29, 2009, Tiversa CEO Robert Boback testified about the Open Door Clinic leak before the Committee. Boback stated that 184 Open Door patients were "now victims of identity

³⁰⁹ E-mail from Chris Gormley, COO, Tiversa, to Katy Everett, Tiversa (July 3, 2008, 11:26 a.m.) [hereinafter July 3 Tiversa E-mail].

³¹⁰ Tiversa, *Forensic Investigation Report: Open Door Clinic*, at 6, 21, 26, 29 (Oct. 13, 2011). One of the excerpted documents in the Investigative Report discusses the SISTA Training Institute, and refers participants to the website www.effectiveinterventions.org – the same main website as the link in Gormley's July 3, 2008 e-mail (July 3 Tiversa E-mail).

theft.”³¹¹ After this hearing, a Committee staffer expressed concern to Boback that the affected Open Door clients had not been notified that their personal information had been exposed.³¹²

Rather than contacting the Open Door Clinic to provide additional information about the leak that Tiversa initially withheld, such as the IP address of the source computer, the additional files that Tiversa downloaded, or any investigation Tiversa performed into the identity of the disclosing source, Boback provided information on the Open Door leak to Michael Bruzzese, one of Tiversa’s attorneys.³¹³ Shortly after the July 2009 hearing, Boback provided Bruzzese with a verbal summary of what he knew about the Open Door leak.³¹⁴ Boback also provided one of the six documents Tiversa downloaded from the clinic.³¹⁵ At this time, Boback stated that Tiversa had also determined that an “information aggregator” located in Apache Junction, Arizona downloaded Open Door’s documents.³¹⁶ Boback did not provide Bruzzese with information about any other spread at this time.³¹⁷ Boback also did not provide the Open Door Clinic with information about the alleged spread of the file.

Bruzzese and his co-counsel “retained the services of an attorney who devotes his practice to matters involving legal ethics and the rules of professional responsibility to provide us legal advice as to how and in what manner we could solicit potential clients for this case.”³¹⁸ Bruzzese determined that “it was permitted to contact the potential class members by mail” and sent letters to all patients on the list Boback provided.³¹⁹ The letter was a “solicitation to provide legal services,” and asked the recipient to sign on as a class representative for the suit.³²⁰

Tiversa, through one of its current attorneys, explained to the Committee why Tiversa provided information to Bruzzese instead of contacting Open Door or its patients directly. The attorney stated that Tiversa did not have the resources to contact the patients itself, and accordingly provided the information to an attorney:

³¹¹ *Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security: Hearing Before the H. Comm. on Oversight & Gov’t Reform*, 111th Cong. 12 (July 29, 2009) (testimony of Robert Boback, CEO of Tiversa, Inc.). Michael Bruzzese, however, told the Committee that he did not know what would have been the basis of this statement; he was not aware of any claims of identity theft until after he assembled plaintiffs for the class action lawsuit between November 2009 and February 2010. *H. Comm. on Oversight & Gov’t Reform, Transcribed Interview of Michael Bruzzese*, at 115 (Sept. 10, 2014) [hereinafter Bruzzese Tr.].

³¹² Letter from Michael J. Bruzzese, Att’y, Johnson, Bruzzese & Temple, LLC, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov’t Reform 2 (July 30, 2014) [hereinafter July 30 Bruzzese Letter].

³¹³ *Id.*

³¹⁴ Bruzzese Tr. at 21-22.

³¹⁵ *Id.* at 22.

³¹⁶ *Id.* at 32. A draft version of the Tiversa Forensic Investigation Report includes a file spread analysis. This analysis indicates that the file spread to four IP addresses unrelated to the initial disclosing source. The spread analysis shows that, in addition to the Apache Junction user, a peer-to-peer user in the Netherlands had also downloaded at least one of the Open Door files on March 12, 2009. It is not clear how Boback knew about the spread of the file in one instance, but not the other. Tiversa, *Forensic Investigation Report: Open Door Clinic* (Oct. 21, 2011) (draft report). At no point was Tiversa’s file spread analysis provided to the Open Door Clinic.

³¹⁷ Bruzzese Tr. at 32-33.

³¹⁸ July 30 Bruzzese Letter at 2.

³¹⁹ *Id.*; see also Letter from Michael Bruzzese & James Cirilano, Cirilano & Associates, to [Open Door Clinic Patient] (Nov. 4, 2009) [hereinafter Bruzzese Patient Letter].

³²⁰ Bruzzese Patient Letter..

Here's what our understanding is. And, again, I think you're going to get a letter. . . . Tiversa found the Open Door file. They called them, as is their policy, just saying, look, we found this on your system, here it is. They said, no, thanks, about getting help.

Getting ready for the testimony in 2009, they told the story to someone on staff. And when they told them the story, they were told back that somebody needs to reach out to the victims.

Tiversa did not have the resources to do it themselves, and they just gave a file to the local Pittsburgh attorney, who they knew, in order to help the victims. And Tiversa didn't get any payment for it.³²¹

He further stated:

Well, what he did with it, I don't think -- Tiversa didn't say, go do this or that. It was, they were asked by staff to make sure the victims knew that their information was compromised. **And since they didn't have the ability to do it themselves, or more than what they did, they gave the information to this guy, and he said he would handle it.**³²²

Bruzzese also explained to the Committee how he contacted the clients of the Open Door Clinic. He stated:

Q. How did you contact [the Open Door clients]?

A. We contacted them one way, the only way, by sending them what in our profession is called an attorney solicitation letter, and prior to doing that, I retained the services of a lawyer in Pittsburgh who kind of concentrates his area of practice on professional responsibility and ethics and asked him whether and how under Illinois law that I could contact these individuals. And he did some research, told me **that I was prohibited from making direct phone calls to them but that I could send a letter as long as I marked on the letter that it was a solicitation from a lawyer.** And that's what we did.

* * *

A. Correct. So let me just make a statement to you. **Prior to the five individuals retaining my services as their lawyer, I did not make any telephone calls to any Open Door Clinic patients.**

³²¹ Hopkins Tr.at 143-44.

³²² *Id.* at 145 (emphasis added).

Q. Did you ask Mr. Boback if Tiversa could make telephone calls to any of the Open Door patients?

A. No.

Q. **Did you ask Mr. Boback to contact the Open Door patients in any way?**

A. **No.**³²³

Documents obtained by the Committee, however, show that Tiversa independently contacted patients of the Open Door Clinic about the leak.³²⁴

As these documents call into question information provided by Tiversa to the Committee, the Committee obtained phone records showing long-distance calls from Tiversa's office during the time in question. **A comparison of the phone records to documents Tiversa downloaded from the Open Door Clinic, which contained patients' personal information, clearly shows that Tiversa called more than 50 patients of the Open Door Clinic between October 29 and November 5, 2009.** Tiversa called at least one patient on multiple occasions. These phone calls from Tiversa took place just days before Bruzzese sent a letter to Open Door patients.

It is not clear why Tiversa provided false information to the Committee about whether the company contacted any Open Door patients. Further, it is not clear why Tiversa lacked the resources to contact Open Door patients, as the company represented to the Committee through its attorney. In fact, Tiversa did contact over 50 patients of the clinic. It is also not clear why Tiversa would contact over 50 patients of the clinic in late October and early November 2009, days before Bruzzese sent a letter to patients of the clinic, and following the Committee staffer's July 2009 alleged notification that patients needed to be notified.

In September 2009, Tiversa again contacted Open Door to report that the breached document was still exposed on the peer-to-peer network.³²⁵ Again, Open Door performed its own investigation of its servers and again found no evidence of any peer-to-peer networks.³²⁶ Tiversa did not tell Open Door that it had referred information about the leak to an attorney, nor did Tiversa provide any of the information previously withheld from the clinic. Although Tiversa professed it was concerned about notifying the patients of Open Door about the leak of personally identifiable information, it still omitted key information.

Six patients agreed to join the class action against the Open Door Clinic, and Bruzzese filed the lawsuit in February 2010. During discovery, Open Door subpoenaed Tiversa and

³²³ Bruzzese Tr. at 35-36 (emphasis added).

³²⁴ See, e.g. e-mail from Barb Cox to David Roesler, Dir., Open Door Clinic (Nov. 5 2009 4:29 p.m.) ("According to [redacted]-tiversa [sic] called him first and asked a ton of questions-did they know that open door had done this etc. I think that Triversa [sic] is affiliated with the law firm and sent them the info they had-I would imagine that they get a finders fee [sic].").

³²⁵ Roesler Testimony, at 25.

³²⁶ *Id.* at 25-26.

finally received the additional files that Tiversa downloaded from the same computer on the same day as the one file it previously provided.³²⁷ This production included information indicating that an IP address in Apache Junction, Arizona, downloaded all six Open Door files.³²⁸ Bruzzese testified to the Committee that he also did not receive a full accounting of all the Open Door files Tiversa downloaded until he received Tiversa's production.³²⁹

After receiving full information from Tiversa, the Open Door Clinic determined that the source of the breach was a computer stolen from the clinic in 2007.³³⁰ Open Door believes that the peer-to-peer software that exposed its patients' personally identifiable information was installed on the computer after it was stolen, and therefore was not a breach of Open Door's network.³³¹

D. Tiversa did not charge Bruzzese for the same information it refused to provide to the Open Door Clinic

Tiversa did not accept payment for any services provided as part of the litigation against the Open Door Clinic.³³² When Boback first told Bruzzese about the Open Door leak, Boback was "adamant"³³³ that Tiversa would provide any required services free of charge:

He said, Tiversa does not want anything. I do not want anything. I am doing this to—words to this effect—discharge my obligation put upon me by the staffer to do something about it. **And he said that, whatever you need, in terms of forensic work, you've got, no matter what.**³³⁴

Pursuant to this professed sense of moral obligation, Tiversa performed forensic analysis of the Open Door Leak. Tiversa examined the source of the leak, including details about the 27 times the IP address shifted, the identity of the leak, and the alleged spread of the leak. Tiversa produced a 42-page forensic investigation draft report,³³⁵ and a 39-page final forensic investigation report³³⁶ for Bruzzese's use in the litigation.

Boback directed that Tiversa expend time and effort to investigate the leak for Bruzzese at no charge. He provided the exact same services to Bruzzese for free that he withheld from the Open Door Clinic. Had Boback really felt a sense of moral obligation to the patients of the Open

³²⁷ *Id.* at 94.

³²⁸ The production included a spreadsheet titled "Open Door Clinic File Listing With Spread" and included a list of files for two IP addresses. One IP address is the disclosing source as identified by Tiversa, and the other IP address at the time resolved to Apache Junction, Arizona. Tiversa Production to Open Door Clinic (Jan. 21, 2011).

³²⁹ Bruzzese Tr. at 34.

³³⁰ Roesler Testimony, at 91.

³³¹ *Id.* at 93.

³³² Bruzzese Tr. at 65-66.

³³³ *Id.* at 65.

³³⁴ *Id.*

³³⁵ Tiversa, *Forensic Investigation Report* (Oct. 13, 2011).

³³⁶ Tiversa, *Forensic Investigation Report* (Oct. 21, 2011)..

Door Clinic, he could have provided these services to the Open Door Clinic. Once again, Tiversa was in a position to help and refused to do so.

According to a whistleblower, Tiversa engaged in numerous attempts to get the Open Door Clinic to pay for its services. When the clinic refused, Tiversa began calling the patients listed on the document it downloaded. Tiversa employees thought that by calling the patients and ginning up the leak, they could scare the clinic into hiring Tiversa. When this plan failed, Boback provided the information to his attorney, Michael Bruzzese, who filed a law suit against the non-profit clinic while Tiversa performed work related to the exposure free of charge to Bruzzese. The clinic was never informed by Bruzzese that Bruzzese received the information from Tiversa.

E. Tiversa provided information on the Open Door Clinic to the FTC

In addition to providing information to assist Bruzzese in his class action lawsuit, Tiversa also provided information on the Open Door Clinic leak to the FTC. Tiversa, through the Privacy Institute, provided all six documents about the clinic to the FTC. As noted above, the spreadsheet Tiversa provided indicated that all six documents were downloaded from the same IP address and disclosed on the same day – June 5, 2008.³³⁷ On January 19, 2010, the FTC sent a letter to Open Door Clinic about the leak.³³⁸ The letter informed the clinic that a file had been exposed on the peer-to-peer network, and noted that the clinic’s failure to prevent the document from leaking could violate federal laws.³³⁹

If Boback was truly motivated to help the patients affected by the Open Door leak, he should have given complete information to Open Door immediately. Instead, Boback withheld critical information about the number of downloaded documents, the IP address of the leak, and any information Tiversa had uncovered about the source of the leak. He referred the leak to an attorney. Even after the referral, Tiversa made unsolicited calls to more than 50 patients of the clinic about the leak for unknown reasons. And, finally, Boback provided the very information and services he denied to the Open Door Clinic for free to the attorney who sued the Open Door Clinic over the leak Tiversa first identified. Boback’s actions toward the Open Door Clinic unfortunately fit a pattern of self-promotion and manipulation, not a heartfelt wish to “discharge [his] obligation” to Open Door’s clients.

VII. Conclusion

The Committee’s investigation raises substantial questions about Tiversa’s business practices. The company’s failure to produce documents responsive to the subpoena hindered the Committee’s investigation. Not only did Tiversa primarily report companies to the FTC that had

³³⁷ Microsoft Excel spreadsheet from Tiversa to FTC, “FTC Final 8-14-09pm.xls” [FTC_PROD0000014].

³³⁸ Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Protection, Federal Trade Comm’n, to Open Door Clinic (Jan. 19, 2014).

³³⁹ *Id.*

refused its services, but it also manipulated its relationship with the FTC—including its knowledge of upcoming investigations—in an attempt to profit from these same companies the second time around. In addition, Tiversa seemingly knew about a breach at the House Ethics Committee nine days before the *Washington Post* reported about the breach. Boback notified LifeLock about the breach and the upcoming article, but failed to notify the House Ethics Committee itself. Boback's communications prior to the publication of the article call into question his claim that he did not act as the *Washington Post's* source. Finally, Boback's actions toward the Open Door Clinic are unethical, and potentially illegal. Boback refused to provide critical information about a leak of incredibly sensitive data. Instead, he reported the clinic to the FTC, provided information on the leak to an attorney, and provided certain services to the attorney free of charge but not to the clinic at all.

Boback's actions on behalf of Tiversa demonstrate that when, in a position to prevent harm to companies or the federal government, he acted to benefit himself and Tiversa. Federal departments and agencies should be aware of these business practices when determining whether to do business with Tiversa.

RX649

EXHIBIT 1

Sep 09 2013

Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated)

Article or Commentary, Breaches

Back in July, I reported that **LabMD had unsuccessfully attempted to sue Tiversa in Georgia** for allegedly stealing its property. At issue was a file containing PHI on 1,178 patients that Tiversa had downloaded as part of a research project after the file was exposed via P2P software on LabMD's system. In its 2009 **press release** on its research, Tiversa did not name LabMD, but the matter **eventually came to the FTC's attention**, who opened an investigation and took LabMD to court when it failed to fully comply with an investigative demand. LabMD was ordered to comply, and in August, the **FTC sued LabMD** for failure to adequately protect consumer information. LabMD **responded forcefully** to the complaint in a press statement, alluding to Tiversa as "Internet trolls." In other statements, they've described Tiversa in other unflattering terms.

Now it seems that Tiversa is suing LabMD. Erin McAuley reports:

A cyber-intelligence company and its CEO sued the author of the book "The Devil Inside the Beltway," claiming it falsely accused them of assisting "abusive government shakedowns" through "government-funded data mining & surveillance."

Tiversa Holding Corp. and its co-founder and CEO Robert Boback sued LabMD Inc. and its CEO/author Michael J. Daugherty, in Federal Court.

Daugherty's book is slated for publication on Sept. 17, by (nonparty) Broadland Press. Advance material published on the Internet identifies Daugherty as the CEO of LabMD.

[...]

Boback and Tiversa claim the book defames them: "In his video 'trailer' for the book, available on Mr. Daugherty's personal website, Mr. Daugherty highlights his position as LabMD's president and CEO and Mr. Daugherty alleges that Tiversa is part of a 'Government Funded Data Mining & Surveillance' scheme that engages in 'Psychological Warfare' and helps to assist in 'Abusive Government Shakedown[s].' See www.michaeljdaugherty.com. More specifically, Mr. Daugherty alleges Tiversa is conducting '300 Million Searches per day' for 'Homeland Security' and the 'Federal Trade Commission.'

Read more on [Courthouse News](#).

Seemingly lost in most of the legal wrangling is the fact that it seems that no one whose data were in the "1718 file" were notified of the P2P exposure under HIPAA because LabMD took the position that no breach (as defined by HIPAA in 2008) had occurred.

So is HHS investigating this at all? HHS has not yet responded to an email sent by PHIprivacy.net inquiring as to whether HHS had ever opened (or concluded) an investigation of this incident. This post will be updated when I receive a reply.

Update: An HHS spokesperson responded to my inquiry with the following statement:

OCR decided not to join FTC in their investigation of these p2p sharings and we did not independently receive complaints. As you note, this was pre-HITECH, so there was and is

Featured Articles

- NHS sells a billion patient records
- Louisiana lawmakers want to keep a state database of people who have medication-induced abortions
- Audit finds high-risk security vulnerabilities in the automated systems used to process Medicaid claims
- WA: Skagit County Government Settles Potential HIPAA Violations

Recent Posts

- Service Coordination Inc. also affected MD Department of Health and Mental Hygiene patients
- Business associate of Maryland Developmental Disabilities Administration hacked in October
- Where there's a breach, there's a lawsuit
- AZ: Hospitalists of Arizona laptop stolen from St. Mary's Hospital contained patient information
- NHS sells a billion patient records
- Leader of Stolen Identity Refund Fraud Ring Sentenced to Jail
- CO: Valley View Hospital hacked; 5400 patients affected
- Meanwhile, in the LabMD case...
- UK: Home care agency warned after vulnerable people's details left in the street
- StayWell breach affects over 12,000; how many more not disclosed (update1)

Recent Comments

- Trish Harkness on Leader of Stolen Identity Refund Fraud Ring Sentenced to Jail
- Dissent on StayWell breach affects over 12,000; how many more not disclosed (update1)
- dewluca on StayWell breach affects over 12,000; how many more not disclosed (update1)

News Sections

Select Category

Archives

Select Month

Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated) » PHIprivacy.net
no obligation on LabMD with respect to our breach notification requirements — whether any exist under state law would be for the state to determine.

Posted by Dissent at 3:32 pm

Tagged with: LabMD

4 Responses to “Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated)”

1. **David Szabo** says:

September 10, 2013 at 2:22 pm

The Interim Final Breach Notification Rule did not become effective until September 2009. So if the breach occurred in 2008, is its unlikely that a report was required.

Dissent says:

September 10, 2013 at 2:40 pm

I suspect you're right, and I had made the same point in my July post about the incident pre-dating HITECH. But those data may now have been in a number of hands since HITECH went into effect, so what then? I would think that the PHI lost any HIPAA protection it might have had once it came into the FTC's hands, but how many parties have had access to the data since September 2009, and should HHS be looking into this?

Dissent says:

September 12, 2013 at 3:36 pm

HHS responded to my inquiry. See the update at the bottom of the post. You were correct.

2. **Doc Sheldon** says:

September 14, 2013 at 5:37 pm

I would think that Tiversa's counsel would have advised Mr. Boback that there's little hope of winning a case claiming slander, libel or defamation, when the subject statements can be proven to be true.

It also seems a bit difficult to base a lawsuit upon statements in a book that hasn't yet been published. I guess I'm just a stickler for details.

Sorry, the comment form is closed at this time.

ICS Collection Service, Inc. press release on data breach affecting University of Chicago Physicians Group patients

Update to the inVentiv/Adheris lawsuit against HHS over prescription refill reminder programs

RX653

Samuel P. Hopkins

Chief Technology Officer

Tiversa, Inc.

The Leader in Information Containment Management

144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

This e-mail message and any attachments contain confidential information from Tiversa, Inc. If you are not the intended recipient, you are hereby notified that disclosure, printing, copying, distribution, or the taking of any action in reliance on the contents of this electronic information is strictly prohibited. If you have received this e-mail message in error, please immediately notify the sender by reply message and then delete the electronic message and any attachments.

RX654

RX1

Testimony Before the House Subcommittee on Commerce, Trade and Consumer Protection

Robert Boback, CEO, Tiversa, Inc.

May 4, 2009

TI  **ERSA.**

Good afternoon Chairman Rush, Ranking Member Radanovich and Distinguished Members of the Subcommittee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

As P2P file-sharing risk continues to be a major security, risk and privacy issue, let me first start by first providing a brief background on peer-to-peer.

It is important to note that the Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

Peer-to-peer networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

- 1 – Planned file sharing – its intended use.
- 2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

P2P networks continue to grow in size and popularity due to the alluring draw of the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie

and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may only want to share their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error; access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have adequately highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads a P2P software program on his/her parents computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software program variants that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program.

This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, and foreign intelligence worldwide.

Today, we would like to provide the committee with concrete examples that show the extent of the security problems that are present on the P2P networks and implications of sharing this type of information. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

Despite the tools that P2P network developers are putting into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the

dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

“By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.”

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the “Inadvertent Sharing via P2P Networks,” during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers in previous hearings, the problem continues to exist. In fact, we will also seek to demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been architected in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previ-

ously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Financial Fraud

In an analysis of these searches, listed below is a small sampling of actual searches issued on P2P networks brief research window in March 2009. The term credit card was used as the filter criteria for the period.

2007 credit card numbers
2008 batch of credit cards
2008 credit card numbers
a&l credit card
aa credit card application
abbey credit cards
abbey national credit card
ad credit card authorization
april credit card information
athens mba credit card payment
atw 4m credit card application
austins credit card info
auth card credit
authorization credit card
authorization for credit card
authorize net credit card
bank and credit card informati
bank credit card
bank credit card information
bank credits cards passwords
bank numbers on credit cards
bank of america credit cards
bank of scotland credit card
bank staffs credit cards only
barnabys credit card personal
bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their

tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases where accountant and tax offices, themselves, are inadvertently disclosing client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately \$35. This is up from approximately \$8-\$10 only a few short years ago. One plausible explanation for rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSN. This is a very important point. Our search data shows that thieves in fact a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her tax return, it will automatically be rejected by the IRS's system as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims only to have the initial victim left to address the problem with the IRS. This is very costly and time consuming to resolve.

Stolen SSNs are also used by illegal aliens as a requirement of their gaining employment here in the United States. This crime has far reaching implications as well as a tremendous tax burden on behalf of the victim.

Medical Fraud

Medical information is also being sought after on P2P networks with alarming regularity. Listed below are some terms issued over the same period regarding medical information.

letter for medical bills
letter for medical bills dr
letter for medical bills etmc
letter re medical bills 10th
ltr client medical report
ltr hjh rosimah medical
ltr medical body4life
ltr medical maternity portland
ltr medical misc portland
ltr orange medical head center
ltr to valley medical
lytec medical billing
medical investigation
medical journals password
medical .txt

medical abuse records
medical abuse
medical abuse records
medical algorithms
medical authorization
medical authorization form
medical autorization
medical benefits
medical benefits plan chart
medical biling
medical billing
medical bill
medical biller resume
medical billig software
medical billing
medical billing windows

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, he or she would then immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which he or she would quickly turn into cash by selling the drugs. This is a very difficult crime to detect as most consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company which only serves to prolong the activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

Searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. In the full year of 2006 and 2007, the average annual rise in the search totaled just over 10%.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings in this testimony would put these corporations at further risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information.

The only correlation that we identified is that the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Child Predation

As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can become even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program.

Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

Examples to follow on subsequent pages...

1	A	B	C	D	E	F	G	H	I	J	K
rowid	patientName	patientAddress	patientLocation	patientSSN	patientPhone	patientAddressLine1	patientCity	patientCode	patientSex	patientBirthDate	patientDaycareCode
75211	HOSPITAL	DANIELLA					HOUSTON	77052	Female	12/4/1978	533.31
75212	HOSPITAL	MARQUEE					BRIDGE CITY	77611	Female	1/28/1973	716.5
75213	HOSPITAL	PAMELA					BRIDGE CITY	77611	Female	2/28/1963	716.5
75214	HOSPITAL	MATHEW					BRIDGE CITY	77611-6600	Male	4/30/1922	812.44
75215	HOSPITAL	JAMES					HIGHLAND	77542	Male	1/21/1938	716.5
75216	HOSPITAL	WILLIAM					DALLAS	75236	Male	11/7/1933	553.3
75217	HOSPITAL	ANDREA					PORT ARTHUR	77662	Female	12/30/1970	228.81
75218	HOSPITAL	BRENT					MIOR	77652	Male	4/05/1977	716.5
75219	HOSPITAL	EBERHARDA					GRAND PRAS	75252	Female	7/34/1945	716.5
75220	HOSPITAL	IRIAN					DALLAS	75236	Male	8/30/1979	716.5
75221	HOSPITAL	JAMES					PORT NECHO	77651	Male	12/22/1977	770.0
75222	HOSPITAL	JOHNNY					HOUSTON	77022	Male	1/28/1950	481.21
75223	HOSPITAL	JOHNNY					DALLAS	75211	Male	12/4/1961	288.52
75224	HOSPITAL	GARY					BRIDGE CITY	77611	Male	11/11/1956	611.71
75225	HOSPITAL	STEVEN					DRANGE	77032	Male	11/23/1962	6.8
75226	HOSPITAL	CARMEN					DALLAS	75234	Female	1/05/1961	716.5
75227	HOSPITAL	GREGORY					PT ARTHUR	77642	Male	7/20/1970	553.1
75228	HOSPITAL	DAVID					DE SOTO	75115	Male	11/15/1964	224.2
75229	HOSPITAL	BHANA					DRANGE	77630	Female	8/9/1978	218.46
75230	HOSPITAL	MICHAEL					PORT ARTHUR	77642	Male	1/9/1970	278.81
75231	HOSPITAL	BURDOLPH					BRIDGE CITY	77611	Male	1/21/1956	288.52
75232	HOSPITAL	YOLANDA					DALLAS	75237	Female	11/20/1970	772.83
75233	HOSPITAL	JOE					DALLAS	75233	Male	3/7/1957	416.81
75234	HOSPITAL	ROSIE					DALLAS	75233	Female	12/26/1994	823.3
75235	HOSPITAL	BYLVIA					HOUSTON	77035	Female	2/4/2000	716.5
75236	HOSPITAL	KATHLEEN					HOUSTON	77035	Male	1/8/1969	221
75237	HOSPITAL	ELVIRA					PORT ARTHUR	77642	Female	5/23/1999	281.81
75238	HOSPITAL	BERRY					HOUSTON	77036	Male	7/27/1992	218.46
75239	HOSPITAL	MICHAEL					DALLAS	75234	Female	1/2/1982	318
75240	HOSPITAL	BERRY					PORT ARTHUR	77642	Male	1/3/1952	224.2
75241	HOSPITAL	CAROL					PORT ARTHUR	77642	Female	11/17/1941	513
75242	HOSPITAL	A					DRANGE	77632	Male	3/19/1936	421
75243	HOSPITAL	CALEB					PORT ARTHUR	77642	Male	2/10/2000	281.81
75244	HOSPITAL	JOSIE					DALLAS	75233	Male	10/11/1987	822.2
75245	HOSPITAL	MARY					DALLAS	75234	Female	1/29/1927	644.9
75246	HOSPITAL	L					DALLAS	75211	Male	4/24/1923	716.5
75247	HOSPITAL	IRIAN					DALLAS	75236	Male	8/30/1979	562
75248	HOSPITAL	PATRICIA					PORT ARTHUR	77642	Female	11/4/1952	218.5
75249	HOSPITAL	MARLENA					HOUSTON	77037	Female	4/21/1961	611.71
75250	HOSPITAL	ERIKOLE					HOUSTON	77038	Male	12/24/1960	278.81
75251	HOSPITAL	EMERALEDA					DALLAS	75211	Female	2/14/1988	564
75252	HOSPITAL	DANIELLA					PORT ARTHUR	77642	Female	2-11-2003	281.81
75253	HOSPITAL	ALESSANDRA					HOUSTON	77037	Female	1/3/1969	716.5
75254	HOSPITAL	JOHN					SABINE PASS	77055	Male	3-11-1963	615.3
75255	HOSPITAL	CARLOS					HOUSTON	77053	Male	4/23/1979	278.81
75256	HOSPITAL	JOYCE					DALLAS	75211	Female	8/17/1933	522.1

4	Last	First	SSN	Taxable?	Degree	School	Major	Division
1000	John			N	Certificate	CFA Institute	CFA	Eastern
1001	Zishan			N	Graduate	NYIT	MBA	Western
1002	David			N	Certificate	CFA Institute	CFA	Western
1003	Anthony			N	Graduate	Stevens Institute	MIS	Eastern
1004	Melissa			N	Certificate	Dowling College	CFP	Eastern
1005	Thomas			N	Certificate	Pace	CFP	Eastern
1006	Mary Unley			N	Certificate	American College	CFP	Eastern
1007	Samuel			N	Certificate	Kaplan University	CFP	Eastern
1008	Sandeep			N	Graduate	Steven Institute	Info Mgmt sys	Eastern
1009	Emilee			N	Certificate	Kaplan	CFP	SouthWest
1010	Scott			N	Certificate	Kaplan	CFP	Western
1011	Darya			N	Undergrad	Montclair State University	Marketing	Eastern
1012	Isaac			N	Certificate	Pace University	CFP	Eastern
1013	Sotland			N	Certificate	Kaplan	CFP	Eastern
1014	James			N	Certificate	Kaplan	CFP	Eastern
1015	Steven			N	Graduate	University of Connecticut	MBA	Eastern
1016	Michael			N	Graduate	Stevens Ins	MIS	Eastern
1017	Alejandra			N	Degree	Pace University	BA	Eastern
1018	Hasan			N	Undergrad	NYU	International MBA	Eastern
1019	Sneh			N	Undergrad	Stevens Institute	MIS	Eastern
1020	Luis			N	Undergrad	Axia College	BA	Eastern
1021	Jared			N	Certificate	Kaplan	CFP	Eastern
1022	Matthew			N	Undergrad	Brooklyn College	Finance	Eastern
1023	Francisco			N	Certificate	CFA Institute	CFA	Eastern
1024	Belinda			N	Undergrad	Universidad	Accounting	PR

I	A	D	C	D	C	F	G	H	Z	AA	AB	AC	AD	AE	AF	
ID Number	SSN	First Name	Middle Name	Last Name	Grade	Birth Date	Sex	Mail City State Zip	Tot Quarters							
1022		HALEY			01	01151911	F	SULPHUR LA 71663								
1023		MADSON			03	11121919	F	SULPHUR LA 71663								
1024		PAQUEL			24	06261913	F	SULPHUR LA 71663								
1025		SHANNON			01	10161919	F	SULPHUR LA 71663								
1026		KAMERYN			01	01102011	F	SULPHUR LA 71663								
1027		KENNEDY			04	07121919	F	SULPHUR LA 71663								
1028		SAMUAL			01	04192011	M	SULPHUR LA 71663								
1029		SHELBY			24	04162013	F	SULPHUR LA 71663								
1030		KERRA			04	02151917	F	SULPHUR LA 71663								
1031		WAKENZIE			02	09192011	F	SULPHUR LA 71663								
1032		DREAHNA			06	05271919	F	SULPHUR LA 71663								
1033		NICHOLAS			06	03101914	M	SULPHUR LA 71663								
1034		DANIELLE			06	05191914	F	SULPHUR LA 71663								
1035		ANABELLE			03	04141919	F	SULPHUR LA 71663								
1036		EMLY			06	09121917	F	SULPHUR LA 71663								
1037		JACKSON			07	11141914	M	SULPHUR LA 71663								
1038		BARAH			06	12151911	F	SULPHUR LA 71663								
1039		ALEXANDER			03	09251919	M	SULPHUR LA 71663								
1040		DALEY			24	07162011	F	VICTOR LA 71663								
1041		BRAYDEN			02	04152011	M	SULPHUR LA 71663								
1042		CHRISTOPHER			01	08122011	M	LAKE CHARLES LA 7								
1043		TRINDEA			04	09252011	F	LAKE CHARLES LA 7								
1044		DOUGLAS			06	11122011	M	SULPHUR LA 71663								
1045		JUSTIN			04	12102017	M	SULPHUR LA 71663								
1046		ALLEN			03	03122019	M	SULPHUR LA 71663								
1047		HANNAH			05	02111917	F	SULPHUR LA 71663								
1048		MITCHELL			07	04131915	M	SULPHUR LA 71663								
1049		LAMIC			04	01232011	F	SULPHUR LA 71663								
1050		JENNIFER			06	11121919	F	SULPHUR LA 71663								
1051		JUSTINE			01	11152011	F	SULPHUR LA 71663								
1052		KATE			01	03272011	F	SULPHUR LA 71663								
1053		RYLEE			25	03222012	F	SULPHUR LA 71663								
1054		TANNER			02	12111919	M	SULPHUR LA 71663								
1055		EMMA			07	12131919	F	SULPHUR LA 71663								
1056		MARY			08	12201917	F	SULPHUR LA 71663								
1057		RACHEL			06	01191917	F	SULPHUR LA 71663								
1058		BARAH			16	05111914	F	SULPHUR LA 71663								
1059		AWBER			01	09152011	F	SULPHUR LA 71663								
1060		ASHLEY			01	09252011	F	SULPHUR LA 71663								

I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ID Number	Portford	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One	Bank One
42311	42170	7104	Bank One	11111419	David	G W		CHICAGO	IL	60621	7017				
42312	42171	7104	Bank One	11111419	Jenna R			MENLOYS CORNER	SC	29461	7016				
42313	42172	7104	Bank One	11111419	Mary			UTICA	NY	13101	7011				
42314	42173	7104	Bank One	11111419	Clarence			HAMPTON	VA	23064	7412				
42315	42185	7104	Bank One	11111419	Robert H			WAYNE	PA	19107	7512				
42316	42187	7104	Bank One	11111419	David A			HUMMELSTOWN	PA	17111	7112				
42317	42191	7104	Bank One	11111419	Joseph			NEW SMYRNA BEACH	FL	32181	7016				
42318	42192	7104	Bank One	11111419	Harold			YONERS	NY	14712	7411				
42319	42193	7104	Bank One	11111419	Susan H			COLGNE	TU	40113					
42320	42194	7104	Bank One	11111419	James M			PITTSBURGH	PA	15214	7011				
42321	42195	7104	Bank One	11111419	John J			WARWICK	RI						
42322	42196	7104	Bank One	11111419	Debra M			HENDERSONVILLE	NC	27911	7010				
42323	42197	7104	Bank One	11111419	Ernie L			CHARLESTON	SC	29412	7212				
42324	42198	7104	Bank One	11111419	Janice L			DOTHAN	AL	36101	7011				
42325	42199	7104	Bank One	11111419	James Earl			MILBROOK	AL	36102	7013				
42326	42200	7104	Bank One	11111419	Harold Lee			JACKSONVILLE	FL	32211					
42327	42201	7104	Bank One	11111419	Gregory B			PENSACOLA	FL	32511	7013				
42328	42202	7104	Bank One	11111419	Gregory B			MAMI	FL	33101	7010				
42329	42203	7104	Bank One	11111419	E			MARINA	GA	31402					
42330	42204	7104	Bank One	11111419	Jayna A			MAMI	FL	33144	7014				
42331	42205	7104	Bank One	11111419	Andrew M			PALMBAY	FL	32901	7012				
42332	42206	7104	Bank One	11111419	Steven R			ANCHORAGE	AK	99501	7010				
42333	42207	7104	Bank One	11111419	Carol R			SUNFLOWER	AZ	85121					
42334	42208	7104	Bank One	11111419	Ray C			HUMBLE	TX	75040	7110				
42335	42209	7104	Bank One	11111419	Ruferty G			NOFPOK	VA	23101	7410				
42336	42210	7104	Bank One	11111419	John			NORCROSS	GA	30092	7010				
42337	42211	7104	Bank One	11111419	Abdul			VALDOSTA	GA	31601					
42338	42212	7104	Bank One	11111419	Dorothy			COCHITON	NC	27022	7011				
42339	42213	7104	Bank One	11111419	Alfred J			JERSEY CITY	NJ	07310	7010				
42340	42214	7104	Bank One	11111419	Gary R			ROCKDALE	MA	01911	7013				
42341	42215	7104	Bank One	11111419	Trinity D			CHENAY	OH	43011	7414				
42342	42216	7104	Bank One	11111419	Eric B			MARSHALL	MI	49251	7010				
42343	42217	7104	Bank One	11111419	Nathanael A			DAYVILLE	CA	95521	7010				
42344	42218	7104	Bank One	11111419	Lee T			HUNTERDALE	FL	34142	7110				
42345	42219	7104	Bank One	11111419	Ekraal			SANTA CLARA	CA	95051	7010				
42346	42220	7104	Bank One	11111419	Karen D			HOCKBETT	NH	03101	7014				
42347	42221	7104	Bank One	11111419	Armenian			NORTH MAINE	FL	32101	7012				
42348	42222	7104	Bank One	11111419	Joan			MONTGOMERY	AL	36111	7012				
42349	42223	7104	Bank One	11111419	Dorothy			ORALOGIA	FL	32151	7410				
42350	42224	7104	Bank One	11111419	Barbara			DEERFIELD BEACH	FL	33441	7010				
42351	42225	7104	Bank One	11111419	Edna M			HOMESTEAD	FL	33011	7014				
42352	42226	7104	Bank One	11111419	Nancy J			HALEAH	FL	33112	7019				
42353	42227	7104	Bank One	11111419	Lorna M			LAUDERHILL	FL	33111	7014				
42354	42228	7104	Bank One	11111419	Ernest L			DEERFIELD BEACH	FL	33441	7013				
42355	42229	7104	Bank One	11111419	William			GARFIELD HEIGHTS	OH	44101	7015				
42356	42230	7104	Bank One	11111419	Myrtles C			DAYTONA BEACH	FL	32121	7410				

Tiversa engaged in research involving over 30,000 consumers and found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the last 60 days (2/25-4/26), Tiversa has downloaded 3,908,060 files that have been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. Its important to note that these files were only downloaded with general industry terms and client filters running. Much more exists on the network in a given period of time.

This risk also extends to the military and to overall national security. Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of in excess of 200,000 of our troops.

This issue poses a national security risk. In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the Wall Street Journal printed a front cover story that indicated that former Pentagon officials had indicated that spies had downloaded plans for the \$300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Recommendations

Tiversa's focus has been working for several years with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and

protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

Awareness should extend to corporations as well. With consumers being asked to provide PII to employers, banks, accountants, doctors, hospitals, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary state to state and, in our experience, are seldom respected or followed by organizations.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. The breach law will also need to be enforced as many of the disclosing companies disregard the current state laws, if any to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel Disclosures

Congress should vigorously act to protect the safety and identity of our men and women in uniform. Soldiers who have had their information disclosed should be provided comprehensive identity theft protection services so as to prevent and guard against the use of the breached information.

National Security Disclosures

P2P networks should be continuously monitored globally for the presence of any classified or confidential information that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it)

Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask!

Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service

Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The subcommittee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify here today.



TIVERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940-9030 *office*
(724) 940-9033 *fax*
www.tiversa.com

RX656

No platform fees. No data fees. No trade minimums. Get 300 FREE trades + up to \$1,000. >

Ameritrade logo with 'GET STARTED' button and 'important info' link.

COMPUTERWORLD

Security | Software | IT Management | Virtualization | Operating systems | Hardware Systems | Consumer Electronics | Internet | Telecommunication

IDG News Service >

Innhold a-à

Submi

FTC seeks extensive information from firms being investigated for P2P breaches

o Jaikumar Vijayan 26.02.2010 kl 00.15 |

Tweet 0

Several companies being investigated by the FTC for inadvertently exposing customer and employee data on peer-to-peer networks, have been asked by the agency to submit extensive information on their data-collection, usage and protection practices.

Next Generation In-Memory >

Fast Answers. Simply Delivered. Analytics For The NOW Business

Several companies being investigated by the Federal Trade Commission for inadvertently exposing customer and employee data on peer-to-peer (P2P) networks, have been asked by the agency to submit extensive information on their data-collection, usage and protection practices.

A redacted copy of a request for such information, which the FTC sent to a company that's under investigation, was obtained by Computerworld. It showed the agency is seeking information, dating back to mid-2007, on a wide-range of technology and process-related topics.

For instance, the FTC is asking for detailed information on the types of personal information being collected by the company, the purpose for which it is being used, and how the data is collected, shared and stored.

The letter seeks "detailed descriptions" on how the company compiles, maintains and stores personal information, as well as "high-level diagrams setting out the flow paths" of personal information from source to the point of use.

The company is also required to identify by name, location and operating system every computer that is used to collect and store personal information. In addition, it is required to provide a "narrative" or a blueprint that describes network components in minute detail, down to individual firewalls and routers, and even database tables and field names containing personal data.

The FTC is also requiring any information the company has about its knowledge of the data leaks. The details sought include who knew about the breaches, when, what attempts the company made to inform affected individuals, and why P2P software was allowed to be installed on a company system.

The FTC's 12-page Civil Investigative Demand (CID) letter, which Computerworld viewed, is essentially a federal subpoena that signals the start of a full-fledged federal investigation of a company.

Earlier this week, the FTC announced that it had launched "non-public" investigations against an undisclosed number of companies after discovering they had leaked sensitive personal information on P2P networks.

The companies were targeted for the investigation following a broad FTC probe, during which the agency discovered confidential data from scores of companies available publicly on file-sharing networks.

The data discovered by the FTC included health-related information, financial records, driver's license and Social Security numbers, and other sensitive information belonging to customers and employees at many companies.

In addition to the formal investigations against several companies, the FTC said it had also sent out letters notifying about 100 other companies regarding sensitive and confidential data from their networks being found on publicly available P2P networks.

The notification letters urged the targeted companies to review their security controls and warned them that the data leaks could be putting them in violation of laws enforced by the FTC.

The agency's moves signal what is seen as a long overdue crackdown against companies leaking data on P2P networks. Over the past two years there have been a number of instances of government agencies, businesses and

- Latest news from Government: What does the new EU Parliament mean for tech? (26.05.2014 kl 18:43), Software bug disrupts e-vote count in Belgian election (26.05.2014 kl 13:13), Sony follows Microsoft into Chinese game consoles market (26.05.2014 kl 03:04), Tech giants team up to take on US government gag orders (24.05.2014 kl 22:00), New market of relevance to tech firms: NZX head of markets (23.05.2014 kl 21:38), OGCIO: Hong Kong's IT resources commanders (23.05.2014 kl 18:21)

RX 536

healthcare organizations inadvertently exposing large amounts of personal data as a result of someone improperly installing P2P software on a computer containing the data.

The leaks, some of which have been spectacular, have grabbed the attention of lawmakers, who late last year introduced two bills in Congress aimed at curbing the problem.

The FTC's move shows that the agency is finally exerting its enforcement muscle, said Robert Bobak, CEO of Tiversa Inc., a Cranberry Township, Pa.-based provider of P2P network monitoring services.

"We were happy to see that the FTC [has] finally started recognizing that P2P is a main source for criminals to gain access to consumer's personally identifiable information for ID theft and fraud," Bobak said. Complying with the FTC's request for information could prove to be an "extensive and cumbersome" task for the affected companies, he said.

Between 2001 and last year, the FTC initiated about 25 enforcement actions in total over data breaches involving personal data, Bobak said. That fact that they have now contacted over 100 companies in just the past month is unprecedented and underlines the seriousness with which it is viewing the problem, Bobak said.

Bobak said Tiversa has uncovered as many as 28 million Social Security numbers on P2P networks while performing services for customers. "There are currently thousands of companies that could be receiving letters as the confidential data present remains staggering," he said.

He has testified several times before Congress on the problem of inadvertent data leaks on file-sharing networks, and his company has exposed numerous sensational P2P data breaches over the past few years.

A crackdown by the FTC against those involved in such breaches could benefit companies such as Tiversa, which help businesses figure out if they are leaking protected data on P2P networks. In fact, 14 of the companies contacted by the FTC over the leaks have already contacted Tiversa for help, Bobak said.

"All but two of those have CIDs," he said, adding that complying with the FTC's request for information could prove to be an "extensive and cumbersome" task for the affected companies. "We have confirmed through the companies that have contacted us, that the breaches involve several hundred thousand consumers in total, so far."

Jaikumar Vijayan covers data security and privacy issues, financial services security and e-voting for Computerworld. Follow Jaikumar on Twitter at @jivijayan or subscribe to Jaikumar's RSS feed. His e-mail address is jvijayan@computerworld.com.

Read more about privacy in Computerworld's Privacy Knowledge Center.

Keywords: [Security](#) [Government](#)

[AdChoices](#) [▶ Art News](#) [▶ P2P Music](#) [▶ P2P Sharing](#) [▶ Ares P2P](#)

0 [Tweet](#)

Warning: This comments plugin is operating in compatibility mode, but has no posts yet. Consider specifying an explicit comments plugin documentation to take advantage of all plugin features.

Latest news from IDG News Service

- LG G Flex 2 gets release date and specs: First Android Silver device?
- Coldplay's Ghost Stories soars with album-length animation by Trunk
- What does the new EU Parliament mean for tech?
- Atos offers \$845M for Bull to boost its security and HPC service offering
- WWDC 2014 Apple event: iOS 8, OS X 10.10 coming, new Macs, iWatch, iPhone 6 possible
- Save your Word configurations
- Much more than mixology apps
- Retailers ahead, consumers lagging in mobile payment adoption: Vend
- Landesk acquires LetMobile for secure gateway technology
- Spectrum at the forefront as Telstra's mobile revenue thrives
- Ultra HD, curved screens push 3D out of the spotlight
- ICT outsourcing to veer towards industrialised services: UXC Connect
- Robocop on the beat in Sydney as part of VIVID 2014
- 'Dinosaur' companies don't have agility to compete in Cloud: ServiceNow
- Optus dives into shark detection with Clever Buoy
- Integrated management key to MSPs in Cloud services delivery: GFI Software
- Design a charity poster using Comic Sans to help Cancer Research
- Defined mobility strategies yield better ROI: Bluewolf
- South Korean Kakao messaging app to merge with portal Daum
- New online banking Trojan program combines Zeus and Carberp features
- Software bug disrupts e-vote count in Belgian election

Sony CEO sees wearable gaming gear in company's future
 The philosophy of IoT: Will it help or hurt?
 F5 Networks pounces on fledgling anti-DDoS startup Defense.Net
 Apple asks US court to order Samsung to remove infringing features
 Sony follows Microsoft into Chinese game consoles market
 US seeks leniency for 'Sabu,' Lulzsec leader-turned-snitich
 Apple neglects to renew SSL certificate, breaks Software Update in the process
 Citrix Sharefile to offer meta-data encryption
 Tech giants team up to take on US government gag orders

AdChoices ▶

- ▶ [P2P Music File Sharing](#)
- ▶ [Data Security Breaches](#)
- ▶ [P2P Software](#)

Latest news from IDG News Service

LG G Flex 2 gets release date and specs: First Android Silver device?
 LG brought us teh first curved screen smartphone and the G Flex 2 is rumoured to launch in 2015 and be the first Android Silver device with a Snapdragon 810 64-bit processor.

Coldplay's Ghost Stories soars with album-length animation by Trunk
 Ghost Stories, Coldplay's sixth album, has been given a suitably haunting promo in the shape of an animated album cover by Trunk.

What does the new EU Parliament mean for tech?
 As the dust settles on a new European Parliament, digital rights and IT lobbyists try to work out what it will mean for the tech industry.

Atos offers \$845M for Bull to boost its security and HPC service offering
 French IT services company Atos is seeking to beef up its cybersecurity and high-performance computing offering with a €620 million (US\$845 million) bid for servers and services sp(...)

WWDC 2014 Apple event: iOS 8, OS X 10.10 coming, new Macs, iWatch, iPhone 6 possible
 We know Apple will show off new iOS and OS X features at WWDC 2014, but what else has the company got up its sleeve?



Om IDG Magazines Norge | Annonseinformasjon | Abonnement | Kontaktinformasjon | IDG Internasjonalt | Arkiv

Copyright 2009 IDG Magazines Norge AS. All rights reserved

Barbaks 0000 Contact: 0121 011 01 (Linn) 0121 011 01 (Linn) 0121 011 01 (Linn)

CATEGORY 2

Internal FTC emails and communications regarding OGR's letter of June 11, 2014 to Commissioner Ramirez, and June 17, 2014 to Acting Inspector Gen. Kelly Tshibaka requesting an investigation into FTC and Tiversa in the LabMD matter

RX587



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

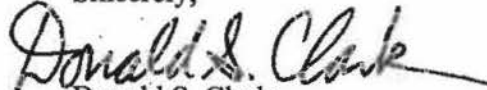
June 13, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
United States House of Representatives
Washington, D.C. 20515-6143

Dear Chairman Issa:

Thank you for your letter to Chairwoman Ramirez dated June 11, 2014 regarding Tiversa, Inc. and information your Committee has obtained from that company. The Federal Trade Commission stands ready to respond to any Committee requests. Because this matter relates to ongoing administrative litigation in *In the Matter of LabMD, Inc., Docket No. 9357*, I am responding on behalf of the agency. Please ask your staff to contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195, if you or your staff have any additional questions.

Sincerely,


Donald S. Clark
Secretary

cc: The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
United States House of Representatives

WAFELLE ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
WILHART N. LUTHER, OHIO
JOHN J. DINGELL, MICHIGAN
PATRICK T. MURPHY, NORTH CAROLINA
JIM JORDAN, OHIO
JASCA CHRISTENSEN, UTAH
TIM WALBERG, MICHIGAN
JAMMIE FRANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICIA MILLER, PENNSYLVANIA
SCOTT DODD, MISSISSIPPI
THEODORE E. SOUZA, CAROLINA
BLAKE FARENTHOLD, TEXAS
DICK HASTINGS, WASHINGTON
CYNTHIA L. LUMMIS, WYOMING
BOB WOODRUFF, GEORGIA
THOMAS MASSIE, KENTUCKY
DUGG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. LENTZ, MICHIGAN
RON DESANTIS, FLORIDA

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MASTERY 1 (202) 225-6711
FACSIMILE (202) 225-3874
MAILING (202) 225-3891
<http://www.house.gov/oversight>

ELIJAH F. CUMMINGS, MARYLAND
RANKING MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN S. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEER, PENNSYLVANIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. ANTHONY LUCCAPORTI, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORNFORD, NEVADA
MICHAEL LUKAN, GEORGIA
NEW MEXICO
WADSWORTH

KENNETH J. BRADY
STAFF DIRECTOR

June 11, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Madam Chairwoman:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company upon which the Federal Trade Commission (“FTC”) relied as a source of information in its enforcement action against LabMD, Inc.¹ Information the Committee recently obtained indicates that the testimony provided by company officials to federal government entities may not have been truthful.

The Committee’s ongoing investigation has shown that competing claims exist about the culpability of those responsible for the dissemination of false information. It is clear at this point, however, that the information provided to the FTC is incomplete and inaccurate. A witness in the proceedings against LabMD, Inc. recently testified to the Committee that he provided incomplete or inaccurate information to the FTC regarding the origin of a “1718” document. In a transcribed interview with Committee staff, Tiversa’s Chief Executive Officer, Robert Boback, testified that he received “incomplete information with regard to my testimony of FTC and LabMD.”² He further stated that the “the original source of the disclosure was incomplete.”³ Mr. Boback testified:

- Q How did you determine that it was incomplete or that there was a problem with the spread analysis?
- A I had . . . [Tiversa Employee A], perform[] an analysis, again, remember, data store versus the peer to peer. So the information in the data store, [Tiversa Employee B] performed another analysis to say, what was the original source of the file from LabMD and what

¹ See *In re LabMD, Inc.*, No. 9357 (Fed. Trade Comm’n Aug. 29, 2013), available at <http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>.

² Transcribed Interview of Robert Boback, Transcript at 129-130 (June 5, 2014) [hereinafter Boback Tr.].

³ *Id.*

The Honorable Edith Ramirez

June 11, 2014

Page 2

was the disclosure, a full analysis of it which then provided to me, which expanded upon what [Tiversa Employee B] had told me when I asked [Tiversa Employee B] prior to my testimony. And the only reason why I asked [Tiversa Employee B] in the first place was because [Tiversa Employee B] was the analyst on it at the time when it was found, so I asked the analyst who was most familiar with this. I didn't know [Tiversa Employee B] was going to provide me with less than accurate information.

* * *

Q So at the time that you were first made aware of the 1718 document in April, May of 2008, Tiversa employees had not conducted the spread analysis?

A No.

Q And you did not know the original source of the 1718 document?

A I did not. No.

* * *

Q Did there come a point at which a Tiversa employee determined who the original source of the 1718 document was?

A Well, that's -- yes. A Tiversa employee told me who the original source was . . . just before I testified . . . in the deposition [in the FTC LabMD case] in November of last year. And, subsequently, we have done a new search and found that the origin was different than what was provided to me . . . in November.

The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony in executive session, and, based on information provided, to immunize certain future testimony pursuant to 18 U.S.C. § 6005. The Committee may request documents and access to relevant FTC witnesses. It is my expectation that you and your staff will cooperate fully with any subsequent requests for documents or transcribed witness interviews.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X.

The Honorable Edith Ramirez
June 11, 2014
Page 3

If you have any questions, please contact the Committee staff at (202) 225-5074.
Thank you for your prompt attention to this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Darrell Issa", written over a horizontal line.

Darrell Issa
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Minority Member
William A. Sherman II, Counsel, LabMD, Inc.
Laura Riposo VanDruff, Complain Counsel, U.S. Federal Trade Commission
William A. Burck, Quinn Emanuel Urquhart & Sullivan LLP

RX592

Kelly, Andrea

From: Hipsley, Heather
Sent: Wednesday, June 18, 2014 12:07 PM
To: Bumpus, Jeanne; Ramirez, Edith; White, Christian S.
Subject: RE: FTC IG has been asked to look into Tiversa matter

Thanks Jeanne; Kelly gave us a heads up and I asked her to double check with Chris when updating us. Thanks, H.

From: Bumpus, Jeanne
Sent: Wednesday, June 18, 2014 11:34 AM
To: Ramirez, Edith; Hipsley, Heather; White, Christian S.
Subject: FTC IG has been asked to look into Tiversa matter

Edith,

Please know that Kelly Tshibaka advised me that she received a letter last night from Chairman Issa asking that the IG look into the Tiversa matter. She could not share the contents of the letter but said it referred also to FTC staff. She will seek to meet with Mr. Issa's staff on the Oversight and Government Reform Committee ASAP and will notify FTC staff of her inquiry.

Jeanne

Kelly, Andrea

From: Tshibaka, Kelly C.
Sent: Wednesday, June 18, 2014 10:51 AM
To: White, Christian S.
Subject: RE: Notice of Request for Investigation

Can you please call me on this when you have a chance?

Kelly Tshibaka
Acting Inspector General
Federal Trade Commission
202-326-3527

From: Hipsley, Heather
Sent: Wednesday, June 18, 2014 10:49 AM
To: Tshibaka, Kelly C.
Cc: White, Christian S.
Subject: RE: Notice of Request for Investigation

Thank you for the heads up; Issa sent a letter to the Chairwoman which asked for our cooperation in any investigation he conducted and Don Clark answered the letter on behalf of the agency since there is a pending administrative litigation related to his concerns. (b)(5)

(b)(5)

(b)(5) Thanks so much, Heather

From: Tshibaka, Kelly C.
Sent: Wednesday, June 18, 2014 10:40 AM
To: Hipsley, Heather
Subject: Notice of Request for Investigation

Heather,

I wanted to let you know that last night we received a request from Chairman Issa to investigate allegations regarding Tiversa and FTC employees' involvement with Tiversa. (b)(5)

(b)(5)

(b)(5) I will keep you posted as this progresses.

Kelly Tshibaka
Acting Inspector General
Federal Trade Commission
202-326-3527

RX593

Kelly, Andrea

From: Clark, Donald S.
Sent: Monday, June 16, 2014 2:50 PM
To: Burstein, Aaron; Davis, Anna; Delaney, Elizabeth A; DeLorme, Christine Lee
Cc: Hipsley, Heather; Bumpus, Jeanne; Vandecar, Kim; White, Christian S.
Subject: Incoming Letter From Chairman Issa and Outgoing Response, Relating To In the Matter of LabMD, Docket No. 9357
Attachments: Issa061314.pdf

Everyone, I've attached a letter from Chairman Issa which relates to the ongoing Part 3 proceeding in In the Matter of LabMD, Inc., Docket No. 9357. (b)(5)
(b)(5)
(b)(5) I've also attached a response we sent to Chairman Issa on Friday, advising him that the FTC stands ready to respond to any Committee requests.

Please let me know if you need any additional information; thanks!

Don



Office of the Secretary

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

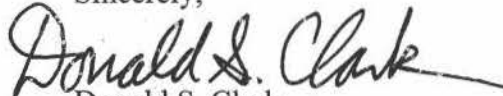
June 13, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
United States House of Representatives
Washington, D.C. 20515-6143

Dear Chairman Issa:

Thank you for your letter to Chairwoman Ramirez dated June 11, 2014 regarding Tiversa, Inc. and information your Committee has obtained from that company. The Federal Trade Commission stands ready to respond to any Committee requests. Because this matter relates to ongoing administrative litigation in *In the Matter of LabMD, Inc.*, Docket No. 9357, I am responding on behalf of the agency. Please ask your staff to contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195, if you or your staff have any additional questions.

Sincerely,


Donald S. Clark
Secretary

cc: The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
United States House of Representatives

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Monday, June 16, 2014 2:30 PM
To: Clark, Donald S.; Vandecar, Kim; White, Christian S.
Subject: RE: Draft Email Message Transmitting Letter From Chairman Issa and Response

Looks good to me Don.

From: Clark, Donald S.
Sent: Monday, June 16, 2014 1:53 PM
To: Bumpus, Jeanne; Vandecar, Kim; White, Christian S.
Subject: FW: Draft Email Message Transmitting Letter From Chairman Issa and Response

..... Jeanne, those are good points! I've tried to incorporate them into the proposed revised response below; (b)(5)
(b)(5)
(b)(5) Please let me know if
this looks OK; thanks!

..... Don

(b)(5)

From: Bumpus, Jeanne
Sent: Monday, June 16, 2014 1:39 PM
To: Clark, Donald S.; Vandecar, Kim; White, Christian S.
Subject: RE: Draft Email Message Transmitting Letter From Chairman Issa and Response

Thanks Don.

(b)(5)

From: Clark, Donald S.
Sent: Monday, June 16, 2014 12:40 PM
To: Bumpus, Jeanne; Vandecar, Kim; White, Christian S.
Subject: Draft Email Message Transmitting Letter From Chairman Issa and Response

LABMD - SUPP. PROD.

Jeanne, Kim and Chris, here's my draft message to the Commissioner Offices; I'd be happy to make any changes you'd like. Thanks!

Don

(b)(5)

From: Clark, Donald S.
Sent: Monday, June 16, 2014 12:16 PM
To: Bumpus, Jeanne
Cc: Vandecar, Kim; White, Christian S.
Subject: RE: Letter from Chairman Issa

Jeanne, thanks; I'll send around the complete package this afternoon; here's a copy of both the incoming letter and the outgoing response, in case you don't have it.

Don

From: Bumpus, Jeanne
Sent: Monday, June 16, 2014 12:06 PM
To: Clark, Donald S.
Cc: Vandecar, Kim; White, Christian S.
Subject: Letter from Chairman Issa

Don,

We have shared the letter dated June 11 from Chairman Issa with the Chairwoman and with Commissioner Ohlhausen's office (who asked for it over the weekend).

(b)(5)

Jeanne

Kelly, Andrea

From: Vandecar, Kim
Sent: Monday, June 16, 2014 12:58 PM
To: White, Christian S.; Clark, Donald S.; Bumpus, Jeanne
Subject: RE: Draft Email Message Transmitting Letter From Chairman Issa and Response

Me too.

From: White, Christian S.
Sent: Monday, June 16, 2014 12:58 PM
To: Clark, Donald S.; Bumpus, Jeanne; Vandecar, Kim
Subject: RE: Draft Email Message Transmitting Letter From Chairman Issa and Response

Looks ok to me.



Kelly, Andrea

From: Davis, Anna
Sent: Sunday, June 15, 2014 10:26 AM
To: Bumpus, Jeanne; White, Christian S.
Subject: Re: Letter from Chairman Issa

Thank you!

From: Bumpus, Jeanne
Sent: Saturday, June 14, 2014 10:48 PM
To: Davis, Anna
Subject: Fw: Letter from Chairman Issa

Anna,
Attached is the letter from Chairman Issa.
Jeanne

From: Oxford, Clinton P.
Sent: Wednesday, June 11, 2014 05:38 PM
To: Bumpus, Jeanne; Vandecar, Kim
Subject: FW: Letter from Chairman Issa

From: Grimm, Tyler [<mailto:Tyler.Grimm@mail.house.gov>]
Sent: Wednesday, June 11, 2014 5:28 PM
To: Oxford, Clinton P.
Cc: Skladany, Jon; Pinto, Ashok; Marin, Mark
Subject: Letter from Chairman Issa
Importance: High

Clinton,

Attached please find a letter from Chairman Issa to Chairwoman Ramirez. Please confirm receipt of this letter.

Tyler Grimm
House Committee on Oversight and Government Reform
Rep. Darrell Issa, Chairman
(202) 225-5074

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Saturday, June 14, 2014 10:43 PM
To: White, Christian S.
Subject: Re: Issa letter

Thanks.

----- Original Message -----

From: White, Christian S.
Sent: Saturday, June 14, 2014 07:39 PM
To: Bumpus, Jeanne; Davis, Anna
Subject: Re: Issa letter

(b)(5)

----- Original Message -----

From: Bumpus, Jeanne
Sent: Saturday, June 14, 2014 08:09 AM
To: Davis, Anna; White, Christian S.
Subject: Re: Issa letter

Anna,

(b)(5)

Jeanne.

----- Original Message -----

From: Davis, Anna
Sent: Friday, June 13, 2014 06:04 PM
To: Bumpus, Jeanne
Subject: Issa letter

Jeanne,

Can you send us a copy of the Issa letter on LabMD?
Anna

Kelly, Andrea

From: Clark, Donald S.
Sent: Friday, June 13, 2014 3:47 PM
To: Hipsley, Heather; White, Christian S.; Vandecar, Kim
Subject: Signed Copy of Letter To Chairman Issa
Attachments: Issa061314.pdf

Heather, thanks for the final version of the letter to Chairman Issa from Edith; I've attached a signed copy (along with a copy of the incoming letter); OCR is delivering the original to Chairman Issa and a copy to Ranking Member Cummings (thanks, Kim!). Please let me know if you need anything else, and everyone have a great weekend!

..... Don



Office of the Secretary

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 13, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
United States House of Representatives
Washington, D.C. 20515-6143

Dear Chairman Issa:

Thank you for your letter to Chairwoman Ramirez dated June 11, 2014 regarding Tiversa, Inc. and information your Committee has obtained from that company. The Federal Trade Commission stands ready to respond to any Committee requests. Because this matter relates to ongoing administrative litigation in *In the Matter of LabMD, Inc.*, Docket No. 9357, I am responding on behalf of the agency. Please ask your staff to contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195, if you or your staff have any additional questions.

Sincerely,

A handwritten signature in black ink that reads "Donald S. Clark".

Donald S. Clark
Secretary

cc: The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
United States House of Representatives

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIN, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DESANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051

<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

June 11, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Madam Chairwoman:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company upon which the Federal Trade Commission ("FTC") relied as a source of information in its enforcement action against LabMD, Inc.¹ Information the Committee recently obtained indicates that the testimony provided by company officials to federal government entities may not have been truthful.

The Committee's ongoing investigation has shown that competing claims exist about the culpability of those responsible for the dissemination of false information. It is clear at this point, however, that the information provided to the FTC is incomplete and inaccurate. A witness in the proceedings against LabMD, Inc. recently testified to the Committee that he provided incomplete or inaccurate information to the FTC regarding the origin of a "1718" document. In a transcribed interview with Committee staff, Tiversa's Chief Executive Officer, Robert Boback, testified that he received "incomplete information with regard to my testimony of FTC and LabMD."² He further stated that the "the original source of the disclosure was incomplete."³ Mr. Boback testified:

- Q How did you determine that it was incomplete or that there was a problem with the spread analysis?
- A I had . . . [Tiversa Employee A], perform[] an analysis, again, remember, data store versus the peer to peer. So the information in the data store, [Tiversa Employee B] performed another analysis to say, what was the original source of the file from LabMD and what

¹ See *In re LabMD, Inc.*, No. 9357 (Fed. Trade Comm'n Aug. 29, 2013), available at <http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>.

² Transcribed Interview of Robert Boback, Transcript at 129-130 (June 5, 2014) [hereinafter Boback Tr.].

³ *Id.*

The Honorable Edith Ramirez
June 11, 2014
Page 2

was the disclosure, a full analysis of it which then provided to me, which expanded upon what [Tiversa Employee B] had told me when I asked [Tiversa Employee B] prior to my testimony. And the only reason why I asked [Tiversa Employee B] in the first place was because [Tiversa Employee B] was the analyst on it at the time when it was found, so I asked the analyst who was most familiar with this. I didn't know [Tiversa Employee B] was going to provide me with less than accurate information.

* * *

Q So at the time that you were first made aware of the 1718 document in April, May of 2008, Tiversa employees had not conducted the spread analysis?

A No.

Q And you did not know the original source of the 1718 document?

A I did not. No.

* * *

Q Did there come a point at which a Tiversa employee determined who the original source of the 1718 document was?

A Well, that's – yes. A Tiversa employee told me who the original source was . . . just before I testified . . . in the deposition [in the FTC LabMD case] in November of last year. And, subsequently, we have done a new search and found that the origin was different than what was provided to me . . . in November.

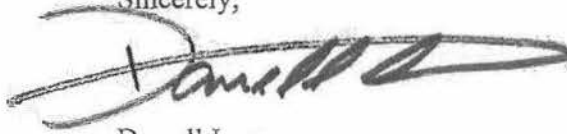
The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony in executive session, and, based on information provided, to immunize certain future testimony pursuant to 18 U.S.C. § 6005. The Committee may request documents and access to relevant FTC witnesses. It is my expectation that you and your staff will cooperate fully with any subsequent requests for documents or transcribed witness interviews.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at “any time” investigate “any matter” as set forth in House Rule X.

The Honorable Edith Ramirez
June 11, 2014
Page 3

If you have any questions, please contact the Committee staff at (202) 225-5074.
Thank you for your prompt attention to this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Darrell Issa", written over a horizontal line.

Darrell Issa
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Minority Member
William A. Sherman II, Counsel, LabMD, Inc.
Laura Riposo VanDruff, Complain Counsel, U.S. Federal Trade Commission
William A. Burck, Quinn Emanuel Urquhart & Sullivan LLP

RX594

Kelly, Andrea

From: Clark, Donald S.
Sent: Friday, June 13, 2014 2:57 PM
To: Hipsley, Heather
Cc: White, Christian S.; Vandecar, Kim
Subject: RE: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Heather, thanks; I just saw your message, as I was in a meeting; I'm signing the letter and taking it to OCR now.

.. Don

From: Hipsley, Heather
Sent: Friday, June 13, 2014 2:06 PM
To: Clark, Donald S.
Cc: White, Christian S.; Vandecar, Kim
Subject: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx
Importance: High

Oops; use this one please. I created a typo in the last version I just sent. Thanks, h.

Kelly, Andrea

From: Hipsley, Heather
Sent: Friday, June 13, 2014 2:05 PM
To: Clark, Donald S.
Cc: Vandecar, Kim; White, Christian S.
Subject: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx
Attachments: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Don, here is the final with Edith's input. Please provide a copy back to our office after you sign and send. Thanks! H.

RX596

Kelly, Andrea

From: Clark, Donald S.
Sent: Thursday, June 12, 2014 11:26 PM
To: Vandecar, Kim; Hipsley, Heather; White, Christian S.
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa

It looks good to me as well; thanks!

Don

From: Vandecar, Kim
Sent: Thursday, June 12, 2014 09:43 PM
To: Hipsley, Heather; Clark, Donald S.; White, Christian S.
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa

Looks good to me.

From: Hipsley, Heather
Sent: Thursday, June 12, 2014 09:33 PM
To: Clark, Donald S.; Vandecar, Kim; White, Christian S.
Subject: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa

Here's what I'll show Edith tomorrow. Any last thoughts? H.

Kelly, Andrea

From: Vandecar, Kim
Sent: Thursday, June 12, 2014 9:31 PM
To: White, Christian S.; Hipsley, Heather; Clark, Donald S.
Cc: Bumpus, Jeanne
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

I like that.

From: White, Christian S.
Sent: Thursday, June 12, 2014 08:55 PM
To: Hipsley, Heather; Clark, Donald S.; Vandecar, Kim
Cc: Bumpus, Jeanne
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

(b)(5)

From: Hipsley, Heather
Sent: Thursday, June 12, 2014 08:52 PM
To: Clark, Donald S.; Vandecar, Kim
Cc: White, Christian S.; Bumpus, Jeanne
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Let me read. I can fix. Thanks h

From: Clark, Donald S.
Sent: Thursday, June 12, 2014 08:18 PM
To: Vandecar, Kim; Hipsley, Heather
Cc: White, Christian S.; Bumpus, Jeanne
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

That's a good point; (b)(5)

Don

From: Vandecar, Kim
Sent: Thursday, June 12, 2014 07:14 PM
To: Clark, Donald S.; Hipsley, Heather
Cc: White, Christian S.; Bumpus, Jeanne
Subject: Re: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Thanks Don. (b)(5)

From: Clark, Donald S.
Sent: Thursday, June 12, 2014 06:44 PM
To: Vandecar, Kim; Hipsley, Heather
Cc: White, Christian S.; Bumpus, Jeanne

Subject: RE: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Kim, those are good points (b)(5)
(b)(5)

..... Don

From: Vandecar, Kim
Sent: Thursday, June 12, 2014 6:17 PM
To: Clark, Donald S.; Hipsley, Heather
Cc: White, Christian S.; Bumpus, Jeanne
Subject: RE: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

(b)(5)

From: Clark, Donald S.
Sent: Thursday, June 12, 2014 6:02 PM
To: Hipsley, Heather
Cc: White, Christian S.; Vandecar, Kim; Bumpus, Jeanne
Subject: RE: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Heather, I've now incorporated Chris's comments; please let us know if you or Edith would like any changes. Thanks!

..... Don

Kelly, Andrea

From: Clark, Donald S.
Sent: Thursday, June 12, 2014 4:52 PM
To: White, Christian S.
Cc: Hipsley, Heather; Bumpus, Jeanne; Vandecar, Kim
Subject: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa
Attachments: Letter To Chairman Issa Acknowledging Receipt of Letter Re Tiversa.docx

Chris, here's the current draft response to Chairman Issa; if it looks OK to you, Heather will forward it on to Edith for review; thanks!

Don

Kelly, Andrea

From: Nuechterlein, Jon
Sent: Thursday, June 12, 2014 12:05 PM
To: Hippsley, Heather
Cc: White, Christian S.
Subject: FW: Letter from Chairman Issa
Attachments: 2014-06-11 DEI to Ramirez-FTC - LabMD Tiversa.pdf

Importance: High

fyi

From: White, Christian S.
Sent: Wednesday, June 11, 2014 6:32 PM
To: Nuechterlein, Jon
Cc: Freedman, Bruce
Subject: FW: Letter from Chairman Issa
Importance: High

Should have copied you.

From: White, Christian S.
Sent: Wednesday, June 11, 2014 6:30 PM
To: Ramirez, Edith
Cc: Bumpus, Jeanne
Subject: FW: Letter from Chairman Issa
Importance: High



From: Bumpus, Jeanne
Sent: Wednesday, June 11, 2014 6:13 PM
To: White, Christian S.
Subject: FW: Letter from Chairman Issa
Importance: High

Chris,

(b)(5)

(b)(5) Would appreciate your advice on how to proceed.. Thanks Chris,

Jeanne

From: Oxford, Clinton P.
Sent: Wednesday, June 11, 2014 5:39 PM
To: Bumpus, Jeanne; Vandecar, Kim
Subject: FW: Letter from Chairman Issa
Importance: High

From: Grimm, Tyler. [<mailto:Tyler.Grimm@mail.house.gov>]
Sent: Wednesday, June 11, 2014 5:28 PM
To: Oxford, Clinton P.
Cc: Skladany, Jon; Pinto, Ashok; Marin, Mark
Subject: Letter from Chairman Issa
Importance: High

Clinton,

Attached please find a letter from Chairman Issa to Chairwoman Ramirez. Please confirm receipt of this letter..

Tyler Grimm
House Committee on Oversight and Government Reform
Rep. Darrell Issa, Chairman
(202) 225-5074

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DESANTIS, FLORIDA

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
<http://oversight.house.gov>

June 11, 2014

LAWRENCE J. BRADY
STAFF DIRECTOR

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Madam Chairwoman:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company upon which the Federal Trade Commission (“FTC”) relied as a source of information in its enforcement action against LabMD, Inc.¹ Information the Committee recently obtained indicates that the testimony provided by company officials to federal government entities may not have been truthful.

The Committee’s ongoing investigation has shown that competing claims exist about the culpability of those responsible for the dissemination of false information. It is clear at this point, however, that the information provided to the FTC is incomplete and inaccurate. A witness in the proceedings against LabMD, Inc. recently testified to the Committee that he provided incomplete or inaccurate information to the FTC regarding the origin of a “1718” document. In a transcribed interview with Committee staff, Tiversa’s Chief Executive Officer, Robert Boback, testified that he received “incomplete information with regard to my testimony of FTC and LabMD.”² He further stated that the “the original source of the disclosure was incomplete.”³ Mr. Boback testified:

- Q How did you determine that it was incomplete or that there was a problem with the spread analysis?
- A I had . . . [Tiversa Employee A], perform[] an analysis, again, remember, data store versus the peer to peer. So the information in the data store, [Tiversa Employee B] performed another analysis to say, what was the original source of the file from LabMD and what

¹ See *In re LabMD, Inc.*, No. 9357 (Fed. Trade Comm’n Aug. 29, 2013), available at <http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>.
² Transcribed Interview of Robert Boback, Transcript at 129-130 (June 5, 2014) [hereinafter Boback Tr.].
³ *Id.*

was the disclosure, a full analysis of it which then provided to me, which expanded upon what [Tiversa Employee B] had told me when I asked [Tiversa Employee B] prior to my testimony. And the only reason why I asked [Tiversa Employee B] in the first place was because [Tiversa Employee B] was the analyst on it at the time when it was found, so I asked the analyst who was most familiar with this. I didn't know [Tiversa Employee B] was going to provide me with less than accurate information.

* * *

Q So at the time that you were first made aware of the 1718 document in April, May of 2008, Tiversa employees had not conducted the spread analysis?

A No.

Q And you did not know the original source of the 1718 document?

A I did not. No.

* * *

Q Did there come a point at which a Tiversa employee determined who the original source of the 1718 document was?

A Well, that's – yes. A Tiversa employee told me who the original source was . . . just before I testified . . . in the deposition [in the FTC LabMD case] in November of last year. And, subsequently, we have done a new search and found that the origin was different than what was provided to me . . . in November.

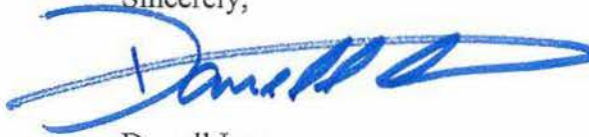
The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony in executive session, and, based on information provided, to immunize certain future testimony pursuant to 18 U.S.C. § 6005. The Committee may request documents and access to relevant FTC witnesses. It is my expectation that you and your staff will cooperate fully with any subsequent requests for documents or transcribed witness interviews.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at “any time” investigate “any matter” as set forth in House Rule X.

The Honorable Edith Ramirez
June 11, 2014
Page 3

If you have any questions, please contact the Committee staff at (202) 225-5074.
Thank you for your prompt attention to this matter.

Sincerely,



Darrell Issa
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Minority Member
William A. Sherman II, Counsel, LabMD, Inc.
Laura Riposo VanDruff, Complain Counsel, U.S. Federal Trade Commission
William A. Burck, Quinn Emanuel Urquhart & Sullivan LLP

Kelly, Andrea

From: Ramirez, Edith
Sent: Wednesday, June 11, 2014 6:32 PM
To: White, Christian S.
Cc: Bumpus, Jeanne
Subject: RE: Letter from Chairman Issa

Chris, thanks.

Duplicate

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Wednesday, June 11, 2014 5:42 PM
To: White, Christian S.
Subject: VM: Bumpus, Jeanne (2946)
Attachments: Voice_Message_Recording_S1186659_001_gsm.wav

»
»
»

RX613

Kelly, Andrea

From: Vandecar, Kim
Sent: Wednesday, June 18, 2014 3:22 PM
To: 'Taylor, Shannon'
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Follow Up Flag: Follow up
Flag Status: Flagged

I'll be in touch shortly.

From: Taylor, Shannon [mailto:shannon.taylor@mail.house.gov]
Sent: Wednesday, June 18, 2014 3:12 PM
To: Vandecar, Kim
Subject: Fw: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

We definitely need to talk now. Let me know if Friday late morning would work. If not we'll find another time.

From: Marrero, Alexa
Sent: Wednesday, June 18, 2014 03:09 PM
To: Nagle, Paul; Taylor, Shannon
Subject: FW: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

ICYMI

From: Watkins, Becca
Sent: Wednesday, June 18, 2014 3:01 PM
Subject: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail



June 18th, 2014
Contact: Becca Watkins, 202.225.0037

Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

WASHINGTON –House Oversight and Government Reform Committee Chairman Darrell Issa, R-Calif., sent a letter to Federal Trade Commission’s (FTC) Acting Inspector General Kelly Tshibaka last night requesting that the IG’s office

LABMD - SUPP. PROD.

0607

4/30/15

investigate the FTC’s relationship with Tiversa, Inc. The Committee has substantial concerns about the reliability of the information Tiversa provided to the FTC and the relationship between the FTC and Tiversa.

In 2008, Tiversa allegedly discovered a document pertaining to LabMD, Inc. containing the personal information of thousands of patients on a peer-to-peer network. Tiversa contacted LabMD in May 2008, explaining that it believed it had identified a data breach at the company and offering “remediation” services through a professional services agreement. LabMD did not accept Tiversa’s offer because LabMD believed it had contained and resolved the data breach. Tiversa, through an entity known as the Privacy Institute, later provided the FTC with a document it created that included information about LabMD, among other companies. Tiversa allegedly provided information to the FTC about companies that refused to buy its services. In the case of LabMD, after Tiversa provided information to the FTC, the Commission sought an enforcement action against the company under its Section 5 authority related to deceptive and unfair trade practices. New information has surfaced indicating that information Tiversa supplied to the FTC may have been inaccurate

“The possibility that inaccurate information played a role in the FTC’s decision to initiate enforcement actions against LabMD is a serious matter,” said Chairman Issa in today’s letter. “The FTC’s enforcement actions have resulted in serious financial difficulties for the company. Additionally, the alleged collaboration between the FTC and Tiversa, a company which has now admitted that the information it provided to federal government entities—including the FTC—may be inaccurate, creates the appearance that the FTC aided a company whose business practices allegedly involve disseminating false data about the nature of data security breaches.”

The letter continues: “Further, the Committee has received information from current and former Tiversa employees indicating a lack of truthfulness in testimony Tiversa provided to federal government entities. The Committee’s investigation is ongoing, and competing claims exist about the culpability of those responsible for the dissemination of false information. It is now clear, however, that Tiversa provided incomplete and inaccurate information to the FTC. “

Read the [letter](#) and embedded below.

June 16, 2014

Ms. Kelly Tshibaka
Acting Inspector General
Federal Trade Commission
Room CC-5206
600 Pennsylvania Avenue NW
Washington, D.C. 20580

Dear Ms. Tshibaka:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company that provided information to Federal Trade Commission in an enforcement action against LabMD, Inc.^[1] In 2008, Tiversa allegedly discovered a document containing the personal information of thousands of patients on a peer-to-peer network.^[2] Tiversa contacted LabMD in May 2008, explaining that it believed it had identified a data breach at the company and offering “remediation” services through a professional services agreement.^[3] LabMD did not accept Tiversa’s offer because LabMD believed it had contained and resolved the data breach. Tiversa, through an entity

known as the Privacy Institute, later provided the FTC with a document it created that included information about LabMD, among other companies.^[4] Apparently, Tiversa provided information to the FTC about companies that refused to buy its services. In the case of LabMD, after Tiversa provided questionable information to the FTC, the Commission sought an enforcement action against the company under its Section 5 authority related to deceptive and unfair trade practices.^[5]

In addition to concerns about the merits of the enforcement action with respect to the FTC’s jurisdiction, the Committee has substantial concerns about the reliability of the information Tiversa provided to the FTC, the manner in which Tiversa provided the information, and the relationship between the FTC and Tiversa. For instance, according to testimony by Tiversa CEO Robert Boback, the Committee has learned of allegations that Tiversa created the Privacy Institute in conjunction with the FTC specifically so that Tiversa could provide information regarding data breaches to the FTC in response to a civil investigative demand. The Committee has also learned that Tiversa, or the Privacy Institute, may have manipulated information to advance the FTC’s investigation. If these allegations are true, such coordination between Tiversa and the FTC would call into account the LabMD enforcement action, and other FTC regulatory matters that relied on Tiversa supplied information.

Further, the Committee has received information from current and former Tiversa employees indicating a lack of truthfulness in testimony Tiversa provided to federal government entities. The Committee’s investigation is ongoing, and competing claims exist about the culpability of those responsible for the dissemination of false information. It is now clear, however, that Tiversa provided incomplete and inaccurate information to the FTC. In a transcribed interview with Oversight and Government Reform Committee staff, Boback testified that he received “incomplete information with regard to my testimony of FTC and LabMD.”^[6] He stated that he now knows “[t]he original source of the disclosure was incomplete.”^[7] Mr. Boback testified:

Q How did you determine that it was incomplete or that there was a problem with the spread analysis?

A I had . . . [Tiversa Employee A] perform[] an analysis, again, remember, data store versus the peer to peer. So the information in the data store, he performed another analysis to say, what was the original source of the file from LabMD and what was the disclosure, a full analysis of it which then provided to me, which expanded upon what [Tiversa Employee B] had told me when I asked [Tiversa Employee B] prior to my testimony. And the only reason why I asked [Tiversa Employee B] in the first place was because [Tiversa Employee B] was the analyst on it at the time when it was found, so I asked the analyst who was most familiar with this. I didn't know [Tiversa Employee B] was going to provide me with less than accurate information.^[8]

* * *

Q So at the time that you were first made aware of the 1718 document in April, May of 2008, Tiversa employees had not conducted the spread analysis?

A No.

Q And you did not know the original source of the 1718 document?

A I did not. No.

* * *

Q Did there come a point at which a Tiversa employee determined who the original source of the 1718 document was?

A Well, that's – yes. A Tiversa employee told me who the original source was ... just before I testified ... in the deposition [in the FTC LabMD case] in November of last year. And, subsequently, we have done a new search and found that the origin was different than what was provided to me . . . in November.^[9]

The possibility that inaccurate information played a role in the FTC’s decision to initiate enforcement actions against LabMD is a serious matter. The FTC’s enforcement actions have resulted in serious financial difficulties for the company.^[10] Additionally, the alleged collaboration between the FTC and Tiversa, a company which has now admitted that the information it provided to federal government entities—including the FTC—may be inaccurate, creates the appearance that the FTC aided a company whose business practices allegedly involve disseminating false data about the nature of data security breaches. The Committee seeks to understand the motivations underlying the relationship between Tiversa and the FTC.

The Committee is currently considering next steps, including the possibility of holding hearings, agreeing to take certain testimony in executive session, and, based on information provided, to immunize certain future testimony pursuant to 18 U.S.C. § 6005. Concurrent with the Committee’s investigative efforts, I request that you undertake a full review of the FTC’s relationship with Tiversa.

Specifically, I ask that your office examine the following issues:

1. FTC procedures for receiving information that it uses to bring enforcement actions pursuant to its authority under Section 5, and whether FTC employees have improperly influenced how the agency receives information.
2. The role played by FTC employees, including, but not limited to, Alain Sheer and Ruth Yodaiken, in the Commission’s receipt of information from Tiversa, Inc. through the Privacy Institute or any other entity, and whether the Privacy Institute or Tiversa received any benefit for this arrangement.
3. The reasons for the FTC’s issuance of a civil investigative demand to the Privacy Institute instead of Tiversa, the custodian of the information.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at “any time” investigate “any matter” as set forth in House Rule X.

If you have any questions about this request, please contact Tyler Grimm or Jennifer Barblan of the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,

Darrell Issa
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

Becca Glover Watkins
Communications Director

LABMD - SUPP. PROD.

0610

4/30/15

House Committee on Oversight and Government Reform
Chairman Darrell Issa
Rayburn 2157
202.731.7234 - Blackberry
202.225.0037 - Press
202.225.5074 - Committee Main
becca.watkins@mail.house.gov
[http:// oversight.house.gov/](http://oversight.house.gov/)

^[1] See Complaint, *In re* LabMD, Inc., No. 9357 (Fed. Trade Comm’n, Aug. 29, 2013), available at <http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>.
^[2] Respondent LabMD, Inc.’s Answer and Defenses to Administrative Complaint, *In re* LabMD, Inc., No. 9357 (Fed. Trade Comm’n, Sept. 17, 2013), at 5.
^[3] Respondent LabMD, Inc.’s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, *In re* LabMD, Inc., No. 9357 (Fed. Trade Comm’n, Nov. 12, 2013), at 5.
^[4] H. Comm. on Oversight & Gov’t Reform, Transcribed Interview of Robert Boback, Chief Executive Officer, Tiversa, Inc., Transcript at 42 (June 5, 2014) [hereinafter Boback Tr.].
^[5] See generally 15 U.S.C. § 45.
^[6] Boback Tr. at 129.
^[7] *Id.*
^[8] *Id.* at 129-130.
^[9] *Id.* at 162-163.
^[10] Rachel Louise Ensign, *FTC Cyber Case Has Nearly Put Us Out of Business, Firm Says*, WALL ST. J., Jan. 28, 2014, <http://blogs.wsj.com/riskandcompliance/2014/01/28/ftc-cyber-case-has-nearly-put-us-out-of-business-firm-says/>.

RX614

Kelly, Andrea

From: Vandecar, Kim
Sent: Wednesday, June 18, 2014 5:27 PM
To: 'Taylor, Shannon'
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Follow Up Flag: Follow up
Flag Status: Flagged

Yes.

From: Taylor, Shannon [mailto:shannon.taylor@mail.house.gov]
Sent: Wednesday, June 18, 2014 5:25 PM
To: Vandecar, Kim
Subject: Re: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

11am on Friday in H2-255?

From: Vandecar, Kim [mailto:KVANDECAR@ftc.gov]
Sent: Wednesday, June 18, 2014 04:10 PM
To: Taylor, Shannon
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

It will... Tell us when and where. Daniel Kaufman, Deputy Director of BCP, will come along with one of our General Counsels, Maneesha, Jeanne and myself.

Duplicate

LABMD - SUPP. PROD.

0612

4/30/15

Kelly, Andrea

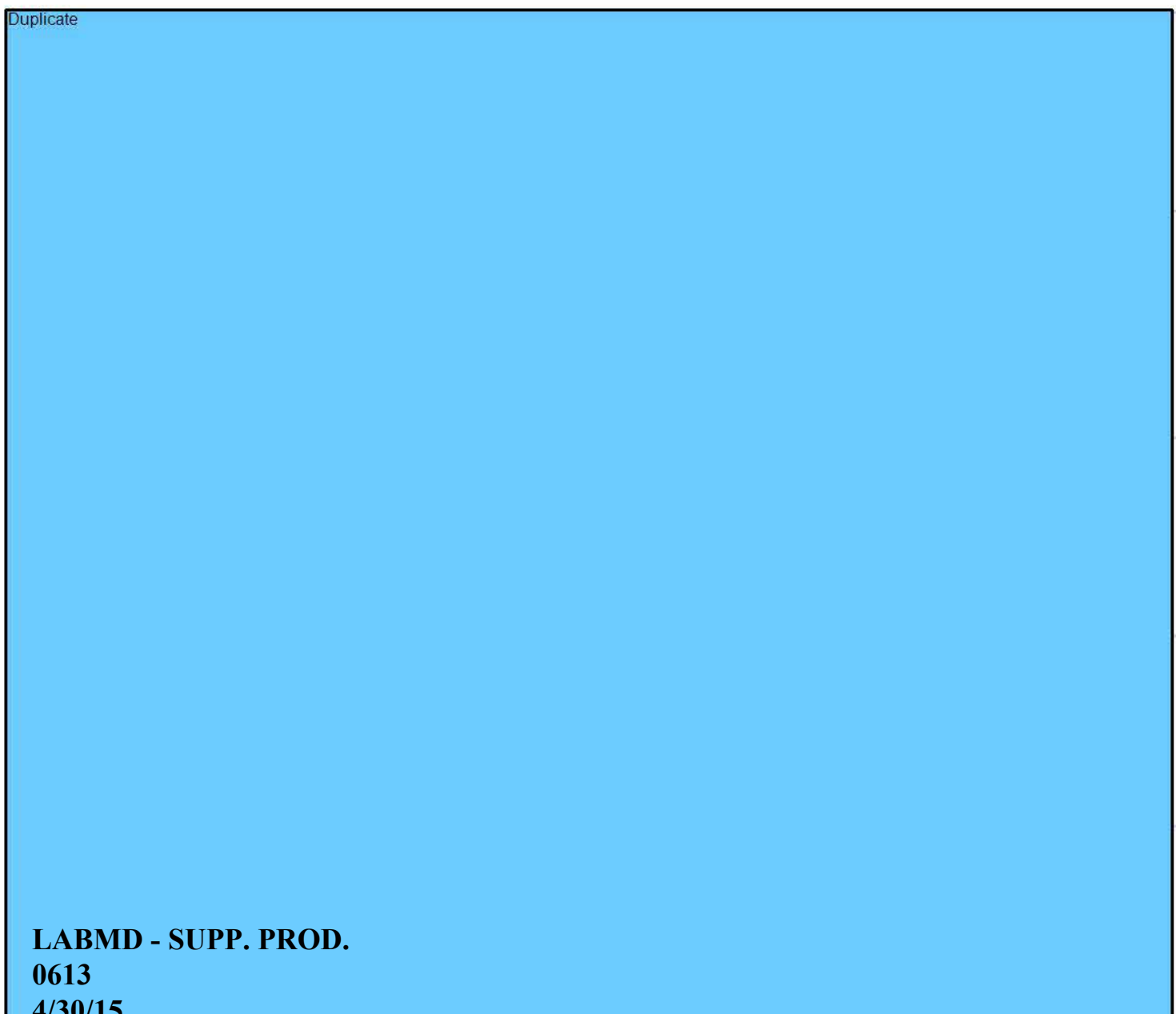
From: Taylor, Shannon <shannon.taylor@mail.house.gov>
Sent: Wednesday, June 18, 2014 5:29 PM
To: Vandecar, Kim
Subject: Re: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Follow Up Flag: Follow up
Flag Status: Flagged

Second floor of ford btwn the elevator banks.

From: Vandecar, Kim [mailto:KVANDECAR@ftc.gov]
Sent: Wednesday, June 18, 2014 05:28 PM
To: Taylor, Shannon
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Where is that?



LABMD - SUPP. PROD.

0613

4/30/15

RX617

Kelly, Andrea

From: Taylor, Shannon <shannon.taylor@mail.house.gov>
Sent: Wednesday, June 18, 2014 12:16 PM
To: Vandecar, Kim
Subject: LabMD/Tiversa/Government Reform

Follow Up Flag: Follow up
Flag Status: Flagged

Hey, Kim.

I've been meaning to reach out to you on this. You guys have any thoughts you want to share with us, or just tell us generally what's happening in this case now that Government Reform is sniffing around Tiversa?

<http://blogs.wsj.com/riskandcompliance/2014/06/03/u-s-lawmakers-investigating-ftcs-use-of-firm-in-data-cases/>

<http://blogs.wsj.com/riskandcompliance/2014/06/12/house-committee-says-ftc-privacy-case-incomplete-and-inaccurate/>

Shannon Taylor
Counsel, Majority Staff
Committee on Energy & Commerce
U.S. House of Representatives
2125 Rayburn HOB/316 Ford HOB
Washington, DC 20515
202.225.2927



RX619

Kelly, Andrea

From: Vandecar, Kim
Sent: Friday, June 13, 2014 3:49 PM
To: 'dave.rapallo@mail.house.gov'; 'susanne.grooms@mail.house.gov'
Cc: Bumpus, Jeanne
Subject: FTC response to Chairman Issa
Attachments: Chairman Issa response.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Good Afternoon,

Attached is the Commission response to Chairman Issa’s letter. Please let me know if you have any questions.

Regards,

Kim Vandecar
202-326-2858



Office of the Secretary

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 13, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
United States House of Representatives
Washington, D.C. 20515-6143

Dear Chairman Issa:

Thank you for your letter to Chairwoman Ramirez dated June 11, 2014 regarding Tiversa, Inc. and information your Committee has obtained from that company. The Federal Trade Commission stands ready to respond to any Committee requests. Because this matter relates to ongoing administrative litigation in *In the Matter of LabMD, Inc., Docket No. 9357*, I am responding on behalf of the agency. Please ask your staff to contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195, if you or your staff have any additional questions.

Sincerely,



Donald S. Clark
Secretary

cc: The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
United States House of Representatives

RX621

Kelly, Andrea

From: Marin, Mark <Mark.Marin@mail.house.gov>
Sent: Friday, June 13, 2014 3:51 PM
To: Vandecar, Kim
Cc: Pinto, Ashok; Skladany, Jon; Bumpus, Jeanne
Subject: Re: FTC response to Chairman Issa

Follow Up Flag: Follow up
Flag Status: Flagged

Thank you, will do.

On Jun 13, 2014, at 3:43 PM, "Vandecar, Kim" <KVANDECAR@ftc.gov> wrote:

Hi Mark,

Attached is the Commission response to Chairman Issa's letter. Let me know if you have any questions.

Regards,

Kim
202-326-2858

<Chairman Issa response.pdf>

Kelly, Andrea

From: Oxford, Clinton P.
Sent: Wednesday, June 11, 2014 5:43 PM
To: 'Grimm, Tyler'
Cc: Skladany, Jon; Pinto, Ashok; Marin, Mark; Vandecar, Kim; Bumpus, Jeanne
Subject: RE: Letter from Chairman Issa

Follow Up Flag: Follow up
Flag Status: Flagged

Tyler,

I have received the letter and will deliver it to the Chairwoman.

Best,

Clinton Oxford
Honors Paralegal
Office of Congressional Relations
Federal Trade Commission
(202) 326-2544
coxford@ftc.gov

From: Grimm, Tyler [<mailto:Tyler.Grimm@mail.house.gov>]
Sent: Wednesday, June 11, 2014 5:28 PM
To: Oxford, Clinton P.
Cc: Skladany, Jon; Pinto, Ashok; Marin, Mark
Subject: Letter from Chairman Issa
Importance: High

Clinton,

Attached please find a letter from Chairman Issa to Chairwoman Ramirez. Please confirm receipt of this letter..

Tyler Grimm
House Committee on Oversight and Government Reform
Rep. Darrell Issa, Chairman
(202) 225-5074

RX622

Kelly, Andrea

From: Wender, Joseph (Markey) <Joseph_Wender@markey.senate.gov>
Sent: Friday, June 13, 2014 5:38 PM
To: Vandecar, Kim
Subject: Re: Data Security Language

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks

Sent from my BlackBerry 10 smartphone on the Verizon Wireless 4G LTE network.

From: Vandecar, Kim
Sent: Friday, June 13, 2014 5:27 PM
To: Wender, Joseph (Markey)
Subject: FW: Data Security Language

The exact language is in the GMR consent attached—I highlighted the sentence (I think page 3). The concept is all through our testimonies as well. See if that helps.

From: Wender, Joseph (Markey) [mailto:Joseph_Wender@markey.senate.gov]
Sent: Friday, June 13, 2014 4:18 PM
To: Vandecar, Kim
Subject: Data Security Language

Kim,

I am looking for good language about what a strong data security standard should look like, and found this at the bottom of the LabMD case (bottom page 7) "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers . .

." <http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>. However, I would like to cite this from another source (not a complaint). Has the FTC used this language somewhere else?

Thanks,

Joey

Joseph Wender
Senior Policy Advisor
Office of Senator Edward J. Markey
218 Russell Senate Office Building
(202) 224-2742
Joseph_Wender@markey.senate.gov

RX625

Kelly, Andrea

From: Vandecar, Kim
Sent: Tuesday, June 17, 2014 10:13 AM
To: 'Mark.Marin@mail.house.gov'
Subject: Re: Request

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks.

From: Marin, Mark [<mailto:Mark.Marin@mail.house.gov>]
Sent: Tuesday, June 17, 2014 10:08 AM
To: Vandecar, Kim
Subject: RE: Request

Kim,

I'm sorry, but as we discussed last week, the Committee's policy is not to release (or allow in camera review of) full transcripts of interviews or depositions during an investigation, mainly to protect the integrity of subsequent interviews. The Committee continues its investigation of Tiversa and will be conducting additional interviews, and therefore we are unable to share more of the transcript at this time.

Best, Mark

From: Vandecar, Kim [<mailto:KVANDECAR@ftc.gov>]
Sent: Monday, June 16, 2014 4:55 PM
To: Marin, Mark
Subject: RE: Request

Any word on our request to see the entire transcript referenced in the letter to Chair?

From: Marin, Mark [<mailto:Mark.Marin@mail.house.gov>]
Sent: Thursday, June 12, 2014 1:20 PM
To: Vandecar, Kim
Subject: Re: Request

Sure, just tried you, you can reach me at 202-226-0022.

On Jun 12, 2014, at 1:16 PM, "Vandecar, Kim" <KVANDECAR@ftc.gov> wrote:

Can you give me a call? I'm at 202-326-2858

Kelly, Andrea

From: Vandecar, Kim
Sent: Wednesday, June 18, 2014 10:37 AM
To: 'Mark.Marin@mail.house.gov'
Subject: Re: Request

Follow Up Flag: Follow up
Flag Status: Flagged

Disregard. Apparently someone was referencing last weeks letter incorrectly.

From: Vandecar, Kim
Sent: Wednesday, June 18, 2014 09:34 AM
To: 'Marin, Mark' <Mark.Marin@mail.house.gov>
Subject: RE: Request

Mark,

Did you send us a new letter yesterday?



CATEGORY 3

**Internal FTC emails and communications
regarding OGR's July 18, 2014 letter to
Commissioner Ramirez, and OGR's July 24,
2014 hearing entitled "The Federal Trade
Commission and its Section 5 Authority:
Prosecutor, Judge, and Jury"**

RX584

Kelly, Andrea

From: Harrison, Lisa M.
Sent: Monday, July 21, 2014 5:26 PM
To: White, Christian S.
Subject: FW: Issa letter

Importance: High

Could you give me a call?
x3204

From: Kaufman, Daniel
Sent: Monday, July 21, 2014 5:17 PM
To: Bumpus, Jeanne; Harrison, Lisa M.; Vandecar, Kim
Subject: FW: Issa letter

FYI.

From: Kaufman, Daniel
Sent: Monday, July 21, 2014 9:29 AM
To: Kestenbaum, Janis; Davis, Anna; Chilson, Neil; Burstein, Aaron
Cc: Delaney, Elizabeth A; DeLorme, Christine Lee
Subject: RE: Issa letter

(b)(5)



(b)(5) I'd be glad to talk to anyone about what's going on here..

Thanks
Daniel

From: Kaufman, Daniel
Sent: Monday, July 21, 2014 9:23 AM
To: Kestenbaum, Janis; Davis, Anna; Chilson, Neil; Burstein, Aaron
Cc: Delaney, Elizabeth A; DeLorme, Christine Lee
Subject: Issa letter

In case you had not seen the letter. WE are drafting the Commission memo this morning...

Kelly, Andrea

From: Harrison, Lisa M.
Sent: Monday, July 21, 2014 3:57 PM
To: White, Christian S.
Cc: Liu, Josephine
Subject: FW: Signed Copy of Commission Letter To Chairman Issa
Attachments: P034101 Letter Granting Request For Nonpublic Info and Dox Re Tiversa To Chairman Issa.pdf

Commission has approved the request.

From: Clark, Donald S.
Sent: Monday, July 21, 2014 3:55 PM
To: Bumpus, Jeanne; Vandecar, Kim; Mithal, Maneesha; Brin, Katherine Race; Kaufman, Daniel; Harrison, Lisa M.
Cc: Hipsley, Heather; Kestenbaum, Janis; Rich, Jessica L.; Fallow, Katherine; DeMartino, Laura; Frankle, Janice Podoll; Simons, Claudia A.; Runco, Philip; Oxford, Clinton P.
Subject: Signed Copy of Commission Letter To Chairman Issa

..... Everyone, I've attached a scanned copy of the above letter, and we're now bringing the signed original to OCR. Please let us know if you need anything else; thanks!

..... Don



United States of America
 FEDERAL TRADE COMMISSION
 WASHINGTON, D.C. 20580

Office of the Secretary

July 21, 2014

The Honorable Darrell E. Issa
 Chairman
 Committee on Oversight and Government Reform
 United States House of Representatives
 2157 Rayburn House Office Building
 Washington, DC 20515-6143

Dear Chairman Issa:

Thank you for your letter dated July 18, 2014, requesting certain documents. The Commission is responding to your request as an official request of a Congressional Committee, *see* Commission Rule 4.11(b), 16 C.F.R. § 4.11(b), and has authorized its staff to provide the requested documents, along with associated information during discussions.

Most of the documents to be provided to the Committee in response to your request and some of the information that the Commission staff likely would discuss in follow-up conversations are non-public and statutorily protected from public disclosure by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 41 *et seq.* Some of the information may also be exempt from mandatory disclosure under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552.

The responsive documents include highly sensitive personal information about tens of thousands of individuals. Personally identifiable information about individuals is exempt from mandatory public disclosure under Exemption 6 of the Freedom of Information Act, as the disclosure of the information would reasonably be expected to constitute a clearly unwarranted invasion of personal privacy. *See Department of the Air Force v. Rose*, 425 U.S. 352, 372 (1976). In accordance with Commission policies on protecting sensitive personally identifiable information, this information will be encrypted in transit. The Commission requests that the Committee maintain the confidentiality of this information and take appropriate steps to safeguard it.

Some of the documents provided and information that could be discussed would reveal the existence of, and information concerning ongoing, nonpublic law enforcement investigations, including identification of the targets of those investigations. Disclosure of this information reasonably could be expected to interfere with law enforcement proceedings, and this information therefore is protected from mandatory public disclosure by FOIA Exemption 7(A), 5 U.S.C. § 552(b)(7)(A). *See NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 232 (1978); *Ehringhaus v. FTC*, 525 F. Supp. 21, 24 (D.D.C. 1980).

In addition, some of the responsive information and documents may be protected under Section 6(f) of the FTC Act, 15 U.S.C. § 46(f), as confidential commercial or financial information. The Commission is prohibited from disclosing such information publicly, and it would be exempt from disclosure under FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Because disclosure of this information is likely to result in substantial competitive harm to the submitters, or is clearly not of a kind that submitters would customarily make available to the public, it also would be exempt from disclosure under FOIA Exemption 4, 5 U.S.C. § 552(b)(4). *See Critical Mass Energy Project v. NRC*, 975 F.2d 871, 877-80 (D.C. Cir. 1992) (*en banc*), *cert. denied*, 507 U.S. 984 (1993) (exempt status accorded to information submitted voluntarily); *Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974) (exempt status accorded to information submitted under compulsion).

Some of the documents provided and information that could be discussed were obtained by compulsory process or provided voluntarily in lieu thereof in law enforcement investigations. Such information is protected from public disclosure under Section 21(f) of the FTC Act, 15 U.S.C. § 57b-2(f). By virtue of that section, such information also is exempt from public disclosure under FOIA Exemption 3(B), 5 U.S.C. § 552(b)(3)(B). *See McDermott v. FTC*, 1981-1 Trade Cas. (CCH) ¶ 63,964 at 75,982-3 (D.D.C. April 13, 1981); *Dairymen, Inc. v. FTC*, 1980-2 Trade Cas. (CCH) ¶ 63,479 (D.D.C. July 9, 1980).¹

Finally, some of the information that could be discussed and documents to be provided could include internal staff analyses and recommendations, which are pre-decisional, deliberative information and materials exempt from mandatory public disclosure under FOIA Exemption 5, 5 U.S.C. § 552(b)(5). *See NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132 (1975); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980). Some of this information also may be protected from mandatory public disclosure under FOIA Exemption 5 as attorney work product prepared in anticipation of litigation. *See FTC v. Grolier, Inc.*, 462 U.S. 19, 28 (1983); *Martin v. Office of Special Counsel, Merit Systems Protection Bd.*, 819 F.2d 1181, 1187 (D.C. Cir. 1987).

Notwithstanding the protected status of most of the documents and other information that could be discussed, the FTC Act, 15 U.S.C. § 57b-2(d)(1)(A), and the FOIA, 5 U.S.C. § 552(d), provide no authority to withhold such information from this Congressional Committee, and the Commission has authorized staff to provide the documents to Committee staff, along with associated information in any follow-up discussions. Because the confidential information

¹ The Commission is required to notify any person who submitted information pursuant to compulsory process in a law enforcement investigation, if the Commission receives a request from a Congressional Committee or Subcommittee for that information. *See Commission Rule 4.11(b)*, 16 C.F.R. § 4.11(b). Staff will be providing any requisite notice.

would not be available to the public under the FOIA or otherwise, and some of the documents contain highly sensitive personally identifiable information, the Commission requests that the Committee maintain its confidentiality, and take appropriate steps to safeguard the information.

By direction of the Commission.



Donald S. Clark
Secretary

Kelly, Andrea

From: Harrison, Lisa M.
Sent: Monday, July 21, 2014 8:55 AM
To: White, Christian S.
Subject: FW: Letter from Chairman Issa
Attachments: 2014-07-18 DEI to Ramirez-FTC - spreadsheet request.pdf

You already have a copy of the Friday afternoon letter, but I am resending.

-----Original Message-----

From: Shonka, David C.
Sent: Friday, July 18, 2014 4:27 PM
To: Harrison, Lisa M.
Subject: FW: Letter from Chairman Issa

FYI, this is the Issa letter you don't have.

-----Original Message-----

From: Vandecar, Kim
Sent: Friday, July 18, 2014 2:07 PM
To: White, Christian S.; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Rich, Jessica L.; Hipplesley, Heather; Shonka, David C.
Cc: Bumpus, Jeanne
Subject: FW: Letter from Chairman Issa

We have acknowledged receipt. Please let me know if this timetable (Monday at 5:00) is doable.

From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Friday, July 18, 2014 12:28 PM
To: Simons, Claudia A.
Cc: Grimm, Tyler <Tyler.Grimm@mail.house.gov>
Subject: Letter from Chairman Issa

Claudia –

Attached please find a letter from Chairman Issa. Please confirm receipt at your earliest convenience.

Please feel free to call with any questions.

RX584

Thanks,
Jen

Jennifer Barblan

Senior Counsel

Committee on Oversight and Government Reform

Rep. Darrell E. Issa, Chairman

(202) 225-5074

Jennifer.Barblan@mail.house.gov

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DeJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DeSANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

July 18, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Madam Chairwoman:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company the Federal Trade Commission relied upon as a source of information in investigations and enforcement actions. The Committee has learned that the FTC received information on nearly 100 companies from Tiversa, and initiated investigations or enforcement actions against multiple companies after receiving the information. The Committee has received serious allegations against Tiversa related to the ways that the company collected and used that information. In the course of investigating those allegations, the Committee obtained documents and testimony that show the company's business practices cast doubt on the reliability of the information that Tiversa supplied to the FTC. Given what the Committee has learned so far, I have serious reservations about the FTC's reliance on Tiversa as a source of information used in FTC enforcement actions. I am also concerned that the FTC appears to have acted on information provided by Tiversa without verifying it in any meaningful way.

From the information the Committee has gathered the relationship between the FTC and Tiversa dates back to 2007. In July 2007, Tiversa and the FTC testified before the Oversight and Government Reform Committee about the dangers of peer-to-peer networks.¹ Following Tiversa's July 2007 testimony, the FTC had a number of conversations with Tiversa about the risks of inadvertent sharing on peer-to-peer networks.² According to documents obtained by the Committee, after at least two telephone conversations between FTC and Tiversa employees,

¹ H. Comm. on Oversight & Gov't Reform, *Hearing on Inadvertent File Sharing Over Peer-to-Peer Networks*, 110th Cong. (July 24, 2007) (H. Rept. 110-39).

² E-mail traffic indicates that representatives from the FTC and Tiversa held a conference call with an online meeting component on October 26. E-mail from [FTC Employee 1], Fed. Trade Comm'n, to Robert Boback, CEO, Tiversa, Inc. (Oct. 22, 2007 2:23 p.m.) ("We'll plan on speaking with you at 10:30 on Friday morning (10/26). I'll check on our ability to do the call with web access to be able to view a presentation." E-mail from Robert Boback, CEO, Tiversa, Inc., to [FTC Employee 1], Fed. Trade Comm'n (Oct. 22, 2007 3:25 p.m.) ("I have scheduled our demonstration for Friday at 10:30."). Another phone conversation appears to have occurred on December 19, 2007. E-mail from Robert Boback, CEO, Tiversa, Inc., to [FTC Employee 1], Fed. Trade Comm'n (Dec. 11, 2007 2:04 p.m.) ("2 pm on Wednesday (12/19) will work. Let's plan for that time.").

The Honorable Edith Ramirez
 July 18, 2014
 Page 2

Robert Boback, Tiversa's CEO, sent information to the FTC in December 2007.³ It is unclear what specific information Tiversa sent to the FTC at that time or how that information was used.

In 2009, Tiversa and FTC again testified before the Oversight and Government Reform Committee at another hearing on the risk of inadvertent sharing on peer-to-peer networks.⁴ The Committee has learned that around the same time as this hearing, the FTC contacted Tiversa and asked for information about companies with large data breaches.⁵ In order to receive the information, the FTC issued a civil investigative demand to the Privacy Institute, an entity Tiversa apparently created for the specific and sole purpose of providing information to the FTC. Mr. Boback explained the relationship between Tiversa and the Privacy Institute during a transcribed interview with the Committee. He testified that Tiversa lawyers set up the Privacy Institute "to provide some separation from Tiversa from getting a civil investigative demand at Tiversa, primarily. And, secondarily, it was going to be used as a nonprofit, potentially, but it never did manifest."⁶

Through the Privacy Institute, Tiversa produced a spreadsheet to the FTC that contained information on data breaches at a large number of companies.⁷ Mr. Boback further testified that Tiversa provided information on "roughly 100 companies" to the FTC.⁸

In February 2010, the FTC announced that it notified "almost 100 organizations" that personal information had been shared from the organizations' computer networks and was available on peer-to-peer networks.⁹ The FTC also announced that it opened non-public investigations concerning an undisclosed number of companies.¹⁰ The timing of the Privacy Institute's production of negative information on "roughly 100 companies" to the FTC, and the FTC's subsequent announcement that it notified "almost 100 organizations" that they were under FTC scrutiny, creates the appearance that the FTC relied substantially on the information that Tiversa collected and provided.

That same month, Mr. Boback gave an interview to *Computerworld* about the FTC's announcement.¹¹ He stated, "We were happy to see that the FTC [has] finally started recognizing that P2P [peer-to-peer] is a main source for criminals to gain access to consumer's personally identifiable information for ID theft and fraud."¹² Mr. Boback also stated that 14 of the companies the FTC contacted had already reached out to Tiversa for assistance, and that 12

³ E-mail from Robert Boback, CEO, Tiversa, Inc., to [FTC Employee 1], Fed. Trade Comm'n (Dec. 19, 2007 3:08 p.m.) ("Per our discussion...see attached.").

⁴ H. Comm. on Oversight & Gov't Reform, *Hearing on Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security*, 111th Cong. (July 29, 2009) (111-25).

⁵ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback, CEO, Tiversa, Inc., at 169 (June 5, 2014) [hereinafter Boback Tr.].

⁶ Boback Tr. at 42-43.

⁷ Boback Tr. at 169.

⁸ Boback Tr. at 171.

⁹ Fed. Trade Comm'n, Press Release, *Widespread Data Breaches Uncovered by FTC Probe* (Feb. 22, 2010).

¹⁰ *Id.*

¹¹ Jaikumar Vijayan, *FTC seeks extensive information from firms being investigated for P2P breaches*, COMPUTERWORLD, Feb. 25, 2010, http://www.computerworld.com/s/article/9162560/FTC_seeks_extensive_information_from_firms_being_investigat_ed_for_P2P_breaches?taxonomyId=84&pageNumber=1.

¹² *Id.*

The Honorable Edith Ramirez
July 18, 2014
Page 3

of those companies received civil investigative demands.¹³ Because Tiversa was benefiting commercially from the fact that the FTC was investigating the companies that Tiversa itself referred to the FTC, it is critical for the Committee to understand the relationship between the FTC and Tiversa, and whether Tiversa manipulated the FTC in order to enrich themselves.

In order to assist the Committee in its investigation, please provide the following documents as soon as possible, but by no later than 5:00 p.m. on July 21, 2014:

1. All civil investigative demand letters the FTC sent to the Privacy Institute and Tiversa, Inc.
2. All documents, including spreadsheets, produced by the Privacy Institute or Tiversa to the FTC in response to any civil investigative demand letters sent by the FTC.
3. All letters or other notices sent by the FTC sent to “almost 100 organizations” as discussed in a February 22, 2010, FTC press release.
4. All civil investigative demand letters the FTC sent as part of the investigations announced in the February 22, 2010, FTC press release.

The Committee on Oversight and Government Reform is the principal investigative committee of the U.S. House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate “any matter” at “any time.” An attachment to this letter provides additional information about responding to the Committee’s request.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Tyler Grimm or Jennifer Barblan of the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,



Darrell Issa
Chairman

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

¹³ *Id.*

ONE HUNDRED THIRTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

Phone: (202) 225-5224
Fax: (202) 225-5891

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,

CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD, INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.
7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been

located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.

17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.
19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Schedule Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.
5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.

RX586

Kelly, Andrea

From: Harrison, Lisa M.
Sent: Monday, July 21, 2014 8:54 AM
To: Bumpus, Jeanne
Cc: White, Christian S.
Subject: RE:

Thanks, I have the Friday afternoon letter.

-----Original Message-----

From: Bumpus, Jeanne
Sent: Monday, July 21, 2014 8:49 AM
To: Harrison, Lisa M.
Cc: White, Christian S.
Subject:

Lisa,

Attached is the incoming letter from Chairman Issa dated June 11. I have also attached Don's response. In addition, the letter to the IG at <http://oversight.house.gov/wp-content/uploads/2014/06/2014-06-17-DEI-to-Tshibaka-FTC-IG-LabMD-Tiversa.pdf>, and the letter we received Friday afternoon requesting documents, which I will forward separately, provide additional information about what Chairman Issa may be looking into. Of course the title of the hearing "The Federal Trade Commission and its section 5 Authority: Prosecutor, Judge, and Jury" also indicates the scope of Chairman Issa's interests.

Jeanne

RX588

Kelly, Andrea

From: Mithal, Maneesha
Sent: Sunday, July 20, 2014 5:58 PM
To: Harrison, Lisa M.; DeMartino, Laura; Bumpus, Jeanne; White, Christian S.
Subject: Re: Consent for non-public

Laura will send me the model when she gets a chance, and I'll take it from there.

----- Original Message -----

From: Harrison, Lisa M.
Sent: Sunday, July 20, 2014 05:54 PM
To: DeMartino, Laura; Mithal, Maneesha; Bumpus, Jeanne; White, Christian S.
Subject: Fw: Consent for non-public

(b)(5)

----- Original Message -----

From: Bumpus, Jeanne
Sent: Sunday, July 20, 2014 01:40 PM
To: Harrison, Lisa M.; Rich, Jessica L.; Vandecar, Kim; Kaufman, Daniel; Mithal, Maneesha; Schoshinski, Robert; DeMartino, Laura; White, Christian S.; Liu, Josephine
Subject: Re: Consent for non-public

(b)(5)

----- Original Message -----

From: Harrison, Lisa M.
Sent: Sunday, July 20, 2014 01:21 PM
To: Rich, Jessica L.; Vandecar, Kim; Bumpus, Jeanne; Kaufman, Daniel; Mithal, Maneesha; Schoshinski, Robert; DeMartino, Laura; White, Christian S.; Liu, Josephine
Subject: Re: Consent for non-public

(b)(5)

----- Original Message -----

From: Rich, Jessica L.
Sent: Sunday, July 20, 2014 01:14 PM
To: Vandecar, Kim; Bumpus, Jeanne; Kaufman, Daniel; Mithal, Maneesha; Harrison, Lisa M.; Schlueter, Vanessa; Schoshinski, Robert; DeMartino, Laura
Subject: Re: Consent for non-public

Yes
Jessica L. Rich, Director
Bureau of Consumer Protection

Federal Trade Commission

----- Original Message -----

From: Vandecar, Kim
Sent: Sunday, July 20, 2014 01:09 PM
To: Bumpus, Jeanne; Rich, Jessica L.; Kaufman, Daniel; Mithal, Maneesha; Harrison, Lisa M.; Schlueter, Vanessa; Schoshinski, Robert; DeMartino, Laura
Subject: Re: Consent for non-public

Agree completely Jeanne

----- Original Message -----

From: Bumpus, Jeanne
Sent: Sunday, July 20, 2014 01:03 PM
To: Rich, Jessica L.; Vandecar, Kim; Kaufman, Daniel; Mithal, Maneesha; Harrison, Lisa M.; Schlueter, Vanessa; Schoshinski, Robert; DeMartino, Laura
Subject: Re: Consent for non-public

Looping in Laura.

----- Original Message -----

From: Bumpus, Jeanne
Sent: Sunday, July 20, 2014 12:59 PM
To: Rich, Jessica L.; Vandecar, Kim; Kaufman, Daniel; Mithal, Maneesha; Harrison, Lisa M.; Schlueter, Vanessa; Schoshinski, Robert
Subject: Consent for non-public

Sorry for being out of the loop.

(b)(5)

(b)(5)

(b)(5) What do others think?

Jeanne

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Sunday, July 20, 2014 3:00 PM
To: Rich, Jessica L.; Harrison, Lisa M.; Vandecar, Kim; Kaufman, Daniel; Mithal, Maneesha; Schoshinski, Robert; DeMartino, Laura; White, Christian S.; Liu, Josephine
Subject: Re: Consent for non-public

Jessica,

(b)(5)

(b)(5)

Jeanne

----- Original Message -----

From: Rich, Jessica L.
Sent: Sunday, July 20, 2014 02:49 PM
To: Bumpus, Jeanne; Harrison, Lisa M.; Vandecar, Kim; Kaufman, Daniel; Mithal, Maneesha; Schoshinski, Robert; DeMartino, Laura; White, Christian S.; Liu, Josephine
Subject: Re: Consent for non-public

Jeanne (b)(5)

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

Duplicate

Kelly, Andrea

From: Clark, Donald S.
Sent: Saturday, July 19, 2014 7:47 PM
To: DeMartino, Laura; Harrison, Lisa M.
Cc: Hipsley, Heather; Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; Kaufman, Daniel; Schoshinski, Robert; Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: RE: Letter from Chairman Issa
Attachments: (b)(5)

Laura and Lisa, (b)(5)
(b)(5) please let me know if you need anything else. Thanks!

Don

-----Original Message-----

From: Clark, Donald S.
Sent: Saturday, July 19, 2014 6:47 PM
To: Rich, Jessica L.; DeMartino, Laura; Harrison, Lisa M.; Vandecar, Kim; Mithal, Maneesha; Kaufman, Daniel; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

This approach sounds fine, (b)(5)

Don

----- Original Message -----

From: Rich, Jessica L.
Sent: Saturday, July 19, 2014 03:22 PM
To: DeMartino, Laura; Harrison, Lisa M.; Vandecar, Kim; Mithal, Maneesha; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

Thanks!

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

----- Original Message -----

From: DeMartino, Laura
Sent: Saturday, July 19, 2014 01:22 PM
To: Harrison, Lisa M.; Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

(b)(5)

----- Original Message -----

From: Harrison, Lisa M.
Sent: Saturday, July 19, 2014 01:20 PM
To: Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

(b)(5)

(I am in RI with no safe access, back in the office monday morning).

----- Original Message -----

From: Rich, Jessica L.
Sent: Saturday, July 19, 2014 12:25 PM
To: Harrison, Lisa M.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

If someone has a sample, that would be great.
Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

----- Original Message -----

From: Harrison, Lisa M.
Sent: Saturday, July 19, 2014 12:19 PM
To: Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

Depending on what you and heather think is feasible, a short request memo could be sent first thing monday morning with vote requested by the end of the day.

----- Original Message -----

From: Rich, Jessica L.
Sent: Saturday, July 19, 2014 12:16 PM
To: Harrison, Lisa M.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

Yes
Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

----- Original Message -----

RX588

From: Harrison, Lisa M.

Sent: Saturday, July 19, 2014 12:09 PM

To: Vandecar, Kim; Rich, Jessica L.; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather

Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.

Subject: Re: Letter from Chairman Issa

Is any of the material nonpublic?

----- Original Message -----

From: Vandecar, Kim

Sent: Saturday, July 19, 2014 12:07 PM

To: Harrison, Lisa M.; Rich, Jessica L.; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather

Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.

Subject: Re: Letter from Chairman Issa

My understanding is we are going to meet the deadline. But I don't think any of us considered that we would need a vote.

----- Original Message -----

From: Harrison, Lisa M.

Sent: Saturday, July 19, 2014 12:04 PM

To: Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather

Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.

Subject: Re: Letter from Chairman Issa

That said, Josephine and I can work with Laura D. and others on this (Vanessa is out until thursday). As you know, we will need commission approval to release any nonpublic material. Has a decision been made about the deadline?

----- Original Message -----

From: Harrison, Lisa M.

Sent: Saturday, July 19, 2014 10:25 AM

To: Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather

Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine

Subject: Re: Letter from Chairman Issa

(b)(5)

----- Original Message -----

From: Rich, Jessica L.

Sent: Saturday, July 19, 2014 10:05 AM

To: Harrison, Lisa M.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hipsley, Heather

Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine

Subject: Re: Letter from Chairman Issa

But we have Vanessa and Josephine, right?

Jessica L. Rich, Director

Bureau of Consumer Protection

LABMD - SUPP. PROD.

0445

4/30/15

RX588

Federal Trade Commission

----- Original Message -----

From: Harrison, Lisa M.

Sent: Saturday, July 19, 2014 09:40 AM

To: Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Rich, Jessica L.; Hipsley, Heather

Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine

Subject: Re: Letter from Chairman Issa

Just to clarify, this is not the matter Vanessa, Josephine and I have been working on and we don't need to be on the emails.

----- Original Message -----

From: Shonka, David C.

Sent: Friday, July 18, 2014 02:42 PM

To: Vandecar, Kim; White, Christian S.; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Rich, Jessica L.; Hipsley, Heather

Cc: Bumpus, Jeanne; Harrison, Lisa M.; Schlueter, Vanessa; Liu, Josephine

Subject: RE: Letter from Chairman Issa

I will be on travel next week, but please keep me in the loop on this. I will be back in the office on Monday the 28th, looping in Lisa, Vanessa, and Josephine who have been working on this for OGC.

Duplicate

LABMD - SUPP. PROD.

0446

4/30/15

**COA # 000101
FTC-FOIA-2015-00109**

Kelly, Andrea

From: Hipsley, Heather
Sent: Saturday, July 19, 2014 3:14 PM
To: DeMartino, Laura; Harrison, Lisa M.; Rich, Jessica L.; Vandecar, Kim; Mithal, Maneesha; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine; White, Christian S.; Shonka, David C.
Subject: Re: Letter from Chairman Issa

I can get it done on monday. (b)(5)
(b)(5) I can advance tomorrow if its ready and don can send up first thing monday officially. Just let me know if there is anything else I can do. H



Kelly, Andrea

From: Harrison, Lisa M.
Sent: Saturday, July 19, 2014 1:36 PM
To: DeMartino, Laura
Cc: Liu, Josephine; White, Christian S.; Schlueter, Vanessa
Subject: Re: Letter from Chairman Issa

Thanks laura. Can you do a draft of the letter granting the nonpublic and then I can take a look? Are we providing docs that companies or others provided where we need to notify the submitter? I might have a sample of one of those.

Duplicate



Kelly, Andrea

From: Harrison, Lisa M.
Sent: Saturday, July 19, 2014 12:07 PM
To: Nuechterlein, Jon
Cc: Shonka, David C.; White, Christian S.
Subject: Fw: Letter from Chairman Issa
Attachments: 2014-07-18 DEI to Ramirez-FTC - spreadsheet request.pdf

Jon - FYI Chairman Issa is requesting some docs regarding tiversa..

From: Vandecar, Kim
Sent: Friday, July 18, 2014 04:08 PM
To: Harrison, Lisa M.
Subject: FW: Letter from Chairman Issa

From: Simons, Claudia A.
Sent: Friday, July 18, 2014 1:37 PM
To: Vandecar, Kim
Subject: Fw: Letter from Chairman Issa

Do you want me to reply to her and cc you and let her know you are handling?

From: Barblan, Jennifer. [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Friday, July 18, 2014 12:28 PM
To: Simons, Claudia A.
Cc: Grimm, Tyler <Tyler.Grimm@mail.house.gov>
Subject: Letter from Chairman Issa

Claudia -

Attached please find a letter from Chairman Issa. Please confirm receipt at your earliest convenience.

Please feel free to call with any questions.

Thanks,
Jen

Jennifer Barblan
Senior Counsel
Committee on Oversight and Government Reform
Rep. Darrell E. Issa, Chairman
(202) 225-5074
Jennifer.Barblan@mail.house.gov

Kelly, Andrea

From: Rich, Jessica L.
Sent: Saturday, July 19, 2014 10:34 AM
To: White, Christian S.; Harrison, Lisa M.
Subject: RE: Letter from Chairman Issa

Great...

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580

-----Original Message-----

From: White, Christian S.
Sent: Saturday, July 19, 2014 10:33 AM
To: Harrison, Lisa M.; Rich, Jessica L.
Subject: Re: Letter from Chairman Issa

Right, I'll be here next week..

----- Original Message -----

From: Harrison, Lisa M.
Sent: Saturday, July 19, 2014 10:31 AM
To: Rich, Jessica L.
Cc: White, Christian S.
Subject: Re: Letter from Chairman Issa

I believe chris is here next week.

----- Original Message -----

From: Rich, Jessica L.
Sent: Saturday, July 19, 2014 10:30 AM
To: Harrison, Lisa M.; Vandecar, Kim; Mithal, Maneesha; DeMartino, Laura; Kaufman, Daniel; Clark, Donald S.; Schoshinski, Robert; Hippsley, Heather
Cc: Bumpus, Jeanne; Schlueter, Vanessa; Liu, Josephine
Subject: Re: Letter from Chairman Issa

Is chris around next week?.

Jessica L. Rich, Director
Bureau of Consumer Protection
Federal Trade Commission

Duplicate

LABMD - SUPP. PROD.

0457

4/30/15

**COA # 000112
FTC-FOIA-2015-00109**

Kelly, Andrea

From: Shonka, David C.
Sent: Friday, July 18, 2014 4:25 PM
To: Harrison, Lisa M.; White, Christian S.
Cc: Schlueter, Vanessa; Liu, Josephine
Subject: RE: Letter from Chairman Issa

Right -- sorry for the confusion. I was into much of a hurry and confused Issa matters...

-----Original Message-----

From: Harrison, Lisa M.
Sent: Friday, July 18, 2014 3:39 PM
To: Shonka, David C.; White, Christian S.
Cc: Schlueter, Vanessa; Liu, Josephine
Subject: Re: Letter from Chairman Issa

(b)(5)

Duplicate

LABMD - SUPP. PROD.

RX611

Kelly, Andrea

From: Ramirez, Edith
Sent: Wednesday, July 23, 2014 1:53 PM
To: Ellen Doneski
Subject: RE: Rockefeller Letter to Issa Re: Improper Interference

Ellen, thank you for sending a copy of Chairman Rockefeller's letter. -Edith

From: Ellen Doneski
Sent: Wednesday, July 23, 2014 1:34 PM
To: Ramirez, Edith
Subject: Rockefeller Letter to Issa Re: Improper Interference

Senator Rockefeller just sent this letter to Congressman Issa and we wanted to make sure you had a copy. Will call after mark up/hearing on cramming. Best, Ellen

BARBARA BOGGS, CALIFORNIA
BOB CORKER, TENNESSEE
CHRIS COONS, OREGON
DAN COHEN, OHIO
MARK COOPER, ARIZONA
CRAIG DEEM, ILLINOIS
MIKE DEWINE, OHIO
MARK E. DEKRAKER, MISSOURI
DICK DURBIN, IOWA
JIM HATCH, UTAH
JERRY MANLY, MISSISSIPPI
JOHN CORNYN, TEXAS
LINDSEY O'HANRAHAN, ARIZONA
JOHN ROBERTS, MISSISSIPPI
CRAIG ROBERTS, MISSISSIPPI
MICK LEAGAN, MISSISSIPPI
JOHN CORNYN, TEXAS
LINDSEY O'HANRAHAN, ARIZONA
JOHN ROBERTS, MISSISSIPPI
CRAIG ROBERTS, MISSISSIPPI
MICK LEAGAN, MISSISSIPPI

JOHN CORNYN, TEXAS
LINDSEY O'HANRAHAN, ARIZONA
JOHN ROBERTS, MISSISSIPPI
CRAIG ROBERTS, MISSISSIPPI
MICK LEAGAN, MISSISSIPPI
JOHN CORNYN, TEXAS
LINDSEY O'HANRAHAN, ARIZONA
JOHN ROBERTS, MISSISSIPPI
CRAIG ROBERTS, MISSISSIPPI
MICK LEAGAN, MISSISSIPPI

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6126

WEB SITE: <http://commerce.senate.gov>

July 23, 2014

The Honorable Darrell E. Issa
Chairman
U.S. House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Chairman Issa,
Dear Chairman Issa:

I am troubled by the impropriety of your ongoing interference with an administrative trial regarding allegations that the medical testing company LabMD, Inc. (LabMD) violated the security and privacy of almost 10,000 consumers. The trial is the result of an enforcement action brought by the Federal Trade Commission (FTC) against LabMD for lax data-security practices after discovering that consumers' sensitive personal and health information was available through a "peer-to-peer" sharing application and was being used by criminals to commit identity theft. Your interference in this legal matter is apparently going to be the subject of an upcoming hearing on July 24 in the House Committee on Oversight and Government Reform.

You purport to be concerned about allegations that a third-party company provided untruthful testimony to the FTC with regard to the LabMD breach. This allegation would be more properly raised by LabMD's defense counsel to the administrative law judge presiding over this trial. The trial process provides defense counsel with ample opportunity to impugn the veracity or integrity of a witness or evidence. It is not the job of Congress to serve as an advocate for one particular side and attempt to sway a judge who makes determinations of fact based on evidence formally presented under well-established rules and procedures.

Instead of allowing the parties in this trial to present evidence and to argue their positions before an independent fact finder, you are instead using heavy-handed, bullying tactics to undermine due process and to inappropriately assist the defendant, LabMD. As a result of your interference – including a June 11, 2014, letter to Chairwoman Edith Ramirez stating that your Committee may "immunize certain future testimony under 18 U.S.C. § 6005" – the administrative law judge presiding over this case has suspended the trial indefinitely. This delay is completely unnecessary; it needlessly forestalls resolution of this important consumer-protection case.

While Congress obviously has an important role in government oversight, I believe you have overstepped your bounds in this instance. It is not appropriate for Congress to intervene in the midst of a trial and to adversely affect its proceedings, as you have done. The inappropriate

LABMD - SUPP. PROD.

0597

4/30/15

The Honorable Darrell E. Issa

July 23, 2014

Page 2 of 3

timing and nature of your investigation are buttressed by the revelation that LabMD is being represented by a former member of your Committee staff. This raises the question of whether LabMD directly sought your help and intervention in the legal process rather than take the risk of losing on the merits at trial.

Another apparent purpose of your hearing is to express skepticism about the FTC's long-standing and well-established legal authority under Section 5 of the FTC Act to bring an action against companies like LabMD for negligent data-security practices. This skepticism is unfounded, and your public position was recently rejected by a federal judge in the FTC's data security case against Wyndham Corporation. Over the past 13 years, the Commission has initiated dozens of administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and that resulted in improper disclosures of personal information collected from consumers.

Indeed, Congress has mandated that the FTC effectively use its authority to protect consumers from "unfair or deceptive acts or practices in or affecting interstate commerce" – the very issues at the heart of the LabMD case. The legislative history of the FTC Act confirms that Congress intended to delegate broad authority "to the [C]ommission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply... There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." Against this backdrop, one must conclude that your upcoming hearing and current investigation are nothing more or less than an effort to weaken one of our nation's most important consumer-protection laws, a law that has protected generations of American consumers from scams and rip-offs.

Lastly, it is worth noting that due to Congress's repeated failure to pass strong data-security and breach notification legislation, the FTC stands as the primary federal entity protecting American consumers from harmful data breaches. Recent high-profile, large-scale data breaches -- most notably at Target -- have once again raised public awareness about the need for companies to adequately secure consumer information. Because Congress remains incapable of passing meaningful data-security legislation that provides American consumers with strong protections, we must continue to rely on the FTC and its organic authority under the FTC Act to bring enforcement actions against companies that break the law. Rather than continuing to pursue your current course of interference, I would urge you to instead work to pass meaningful data-security legislation. I would welcome your assistance.

As Chairman of the Senate Committee on Commerce, Science, and Transportation, I regard the FTC as the premier consumer-protection agency in the nation. The Commission consistently seeks to carry out its mission of protecting consumers and competition, and the agency and its employees serve as an important watchdog for corporate wrongdoing. If the Commission acted improperly or otherwise relied on faulty testimony or evidence in its case against LabMD, a judge would be the proper arbiter of such an allegation at trial, not Members

RX611

The Honorable Darrell E. Issa

July 23, 2014

Page 3 of 3

of Congress. I urge you to reconsider your actions and to allow for the American legal system and the rule of law – not political theater – to resolve this case.

Sincerely,

A handwritten signature in dark ink, appearing to read "John D. Rockefeller IV", with a long horizontal flourish extending to the right.

John D. Rockefeller IV
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Member

LABMD - SUPP. PROD.

0599

4/30/15

RX612

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Thursday, July 17, 2014 2:24 PM
To: 'Ash, Michelle'; Berroya, Meghan
Subject: RE: hearing

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks Michelle,

Hi Meghan, I would love to talk to you at your earliest convenience. My number is (202) 326-2946.

Jeanne

Jeanne Bumpus
Director
Office of Congressional Relations
Federal Trade Commission
326-2946

From: Ash, Michelle [<mailto:Michelle.Ash@mail.house.gov>]
Sent: Thursday, July 17, 2014 2:21 PM
To: Berroya, Meghan; Bumpus, Jeanne
Subject: hearing

Meghan is with Oversight and Government Reform, Jeanne Bumpus is with FTC congressional. Meet each other. Cheers.

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Monday, July 21, 2014 12:48 PM
To: 'Nagle, Paul'
Subject: RE: Hearing in OGR re: Section 5

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks Paul.

From: Nagle, Paul [<mailto:Paul.Nagle@mail.house.gov>]
Sent: Monday, July 21, 2014 12:48 PM
To: Bumpus, Jeanne
Subject: RE: Hearing in OGR re: Section 5

Thanks for the heads up – that had caught my eye as well. We will monitor the hearing from afar for now.

From: Bumpus, Jeanne [<mailto:JBumpus@ftc.gov>]
Sent: Monday, July 21, 2014 12:19 PM
To: Nagle, Paul
Subject: Hearing in OGR re: Section 5

Paul,

I wanted to make you are aware that the Oversight and Government Reform Committee has noticed a hearing for this Thursday morning entitled “The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury.” We expect they will discuss data security and the LabMD case. We hope to learn more about the hearing this afternoon. ...

Jeanne

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Wednesday, July 23, 2014 2:16 PM
To: Christian Fjeld; Vandecar, Kim
Subject: RE: Letter

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks for sharing it.

From: Christian Fjeld
Sent: Wednesday, July 23, 2014 1:42 PM
To: Bumpus, Jeanne; Vandecar, Kim
Subject: Letter

Jeanne and Kim – attached is a letter that Chairman Rockefeller sent to Chairman Issa with regard to his ongoing investigation and upcoming hearing on LabMD. Call me with any questions.

Christian

Christian Tamotsu Fjeld
Senior Counsel
Senate Committee on Commerce, Science and Transportation
428 Hart Office Building
Washington, DC 20510
p: (202) 224-1270 f: (202) 228-0327

Kelly, Andrea

From: Benway, Kathleen (Commerce) <Kathleen_Benway@commerce.senate.gov>
Sent: Monday, July 21, 2014 9:36 AM
To: Vandecar, Kim; Bumpus, Jeanne; Simons, Claudia A.
Subject: RE: The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury | Committee on Oversight & Government Reform

Follow Up Flag: Follow up
Flag Status: Flagged

I figured

From: Vandecar, Kim [<mailto:KVANDECAR@ftc.gov>]
Sent: Monday, July 21, 2014 9:34 AM
To: Benway, Kathleen (Commerce); Bumpus, Jeanne; Simons, Claudia A.
Subject: RE: The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury | Committee on Oversight & Government Reform

Thanks. We saw it yesterday.

From: Benway, Kathleen (Commerce) [mailto:Kathleen_Benway@commerce.senate.gov]
Sent: Monday, July 21, 2014 9:33 AM
To: Bumpus, Jeanne; Vandecar, Kim; Simons, Claudia A.
Subject: FW: The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury | Committee on Oversight & Government Reform

Link to the Issa hearing is up. No witnesses listed.

<http://oversight.house.gov/hearing/federal-trade-commission-section-5-authority-prosecutor-judge-jury-2/>

RX618



United States of America
 FEDERAL TRADE COMMISSION
 WASHINGTON, D.C. 20580

Office of the Secretary

July 21, 2014

The Honorable Darrell E. Issa
 Chairman
 Committee on Oversight and Government Reform
 United States House of Representatives
 2157 Rayburn House Office Building
 Washington, DC 20515-6143

Dear Chairman Issa:

Thank you for your letter dated July 18, 2014, requesting certain documents. The Commission is responding to your request as an official request of a Congressional Committee, *see* Commission Rule 4.11(b), 16 C.F.R. § 4.11(b), and has authorized its staff to provide the requested documents, along with associated information during discussions.

Most of the documents to be provided to the Committee in response to your request and some of the information that the Commission staff likely would discuss in follow-up conversations are non-public and statutorily protected from public disclosure by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 41 *et seq.* Some of the information may also be exempt from mandatory disclosure under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552.

The responsive documents include highly sensitive personal information about tens of thousands of individuals. Personally identifiable information about individuals is exempt from mandatory public disclosure under Exemption 6 of the Freedom of Information Act, as the disclosure of the information would reasonably be expected to constitute a clearly unwarranted invasion of personal privacy. *See Department of the Air Force v. Rose*, 425 U.S. 352, 372 (1976). In accordance with Commission policies on protecting sensitive personally identifiable information, this information will be encrypted in transit. The Commission requests that the Committee maintain the confidentiality of this information and take appropriate steps to safeguard it.

Some of the documents provided and information that could be discussed would reveal the existence of, and information concerning ongoing, nonpublic law enforcement investigations, including identification of the targets of those investigations. Disclosure of this information reasonably could be expected to interfere with law enforcement proceedings, and this information therefore is protected from mandatory public disclosure by FOIA Exemption 7(A), 5 U.S.C. § 552(b)(7)(A). *See NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 232 (1978); *Ehringhaus v. FTC*, 525 F. Supp. 21, 24 (D.D.C. 1980).

LABMD - SUPP. PROD.

0635

4/30/15

In addition, some of the responsive information and documents may be protected under Section 6(f) of the FTC Act, 15 U.S.C. § 46(f), as confidential commercial or financial information. The Commission is prohibited from disclosing such information publicly, and it would be exempt from disclosure under FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Because disclosure of this information is likely to result in substantial competitive harm to the submitters, or is clearly not of a kind that submitters would customarily make available to the public, it also would be exempt from disclosure under FOIA Exemption 4, 5 U.S.C. § 552(b)(4). See *Critical Mass Energy Project v. NRC*, 975 F.2d 871, 877-80 (D.C. Cir. 1992) (*en banc*), *cert. denied*, 507 U.S. 984 (1993) (exempt status accorded to information submitted voluntarily); *Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974) (exempt status accorded to information submitted under compulsion).

Some of the documents provided and information that could be discussed were obtained by compulsory process or provided voluntarily in lieu thereof in law enforcement investigations. Such information is protected from public disclosure under Section 21(f) of the FTC Act, 15 U.S.C. § 57b-2(f). By virtue of that section, such information also is exempt from public disclosure under FOIA Exemption 3(B), 5 U.S.C. § 552(b)(3)(B). See *McDermott v. FTC*, 1981-1 Trade Cas. (CCH) ¶ 63,964 at 75,982-3 (D.D.C. April 13, 1981); *Dairymen, Inc. v. FTC*, 1980-2 Trade Cas. (CCH) ¶ 63,479 (D.D.C. July 9, 1980).¹

Finally, some of the information that could be discussed and documents to be provided could include internal staff analyses and recommendations, which are pre-decisional, deliberative information and materials exempt from mandatory public disclosure under FOIA Exemption 5, 5 U.S.C. § 552(b)(5). See *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132 (1975); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980). Some of this information also may be protected from mandatory public disclosure under FOIA Exemption 5 as attorney work product prepared in anticipation of litigation. See *FTC v. Grolier, Inc.*, 462 U.S. 19, 28 (1983); *Martin v. Office of Special Counsel, Merit Systems Protection Bd.*, 819 F.2d 1181, 1187 (D.C. Cir. 1987).

Notwithstanding the protected status of most of the documents and other information that could be discussed, the FTC Act, 15 U.S.C. § 57b-2(d)(1)(A), and the FOIA, 5 U.S.C. § 552(d), provide no authority to withhold such information from this Congressional Committee, and the Commission has authorized staff to provide the documents to Committee staff, along with associated information in any follow-up discussions. Because the confidential information

¹ The Commission is required to notify any person who submitted information pursuant to compulsory process in a law enforcement investigation, if the Commission receives a request from a Congressional Committee or Subcommittee for that information. See Commission Rule 4.11(b), 16 C.F.R. § 4.11(b). Staff will be providing any requisite notice.

would not be available to the public under the FOIA or otherwise, and some of the documents contain highly sensitive personally identifiable information, the Commission requests that the Committee maintain its confidentiality, and take appropriate steps to safeguard the information.

By direction of the Commission.



Donald S. Clark
Secretary

RX620

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Monday, July 21, 2014 12:33 PM
To: 'Barblan, Jennifer'; Grimm, Tyler
Cc: Vandecar, Kim
Subject: RE: E-mail addresses

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks. Jessica Rich, Director of our Bureau of Consumer Protection, will join us.

Jeanne

From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Monday, July 21, 2014 12:28 PM
To: Bumpus, Jeanne; Grimm, Tyler
Cc: Vandecar, Kim
Subject: RE: E-mail addresses

We will call you at 2 pm.

Thanks,
Jen

From: Bumpus, Jeanne [<mailto:JBumpus@ftc.gov>]
Sent: Monday, July 21, 2014 11:48 AM
To: Barblan, Jennifer; Grimm, Tyler
Cc: Vandecar, Kim
Subject: RE: E-mail addresses

Thank you,

Yes, 2:00 works for us. Shall we call you or do you want to call us at 326-2946? Kim Vandecar and I will be joined by Daniel Kaufman, who is Deputy Director of the Bureau of Consumer Protection.

Jeanne

From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Monday, July 21, 2014 11:07 AM
To: Bumpus, Jeanne; Grimm, Tyler
Cc: Vandecar, Kim
Subject: Re: E-mail addresses

Thanks Jeanne. Could we speak at 2 this afternoon about the hearing?

From: Bumpus, Jeanne [<mailto:JBumpus@ftc.gov>]
Sent: Monday, July 21, 2014 10:34 AM
To: Barblan, Jennifer; Grimm, Tyler

LABMD - SUPP. PROD.

0640

4/30/15

RX620

Cc: Vandecar, Kim <KVANDECAR@ftc.gov>

Subject: E-mail addresses

Jenn and Tyler,

Wanted to make sure you had our e-mail addresses accessible. We look forward to talking about the hearing this afternoon. Thank you,

Jeanne

RX623

Kelly, Andrea

From: Marin, Mark <Mark.Marin@mail.house.gov>
Sent: Monday, July 21, 2014 5:07 PM
To: Vandecar, Kim
Cc: jennifer.balban@mail.house.gov; Berroya, Meghan; Lessley, Lucinda; Reavis, Brandon; kathleen.peleky@mail.house.gov; Grimm, Tyler; Bumpus, Jeanne; Smith, Matthew
Subject: Re: FTC letter authorizing non-public information to Chairman Issa

Follow Up Flag: Follow up
Flag Status: Flagged

Thank you, Kim.

> On Jul 21, 2014, at 5:04 PM, "Vandecar, Kim" <KVANDECAR@ftc.gov> wrote:
>
> Attached please find the Commission letter authorizing the release of non-public information. Staff at the FTC is working hard to finalize the document transfer. We believe we will have this done no later than 6:00 pm today.
>
> Please let me know if you have any questions.
>
> Best,
>
> Kim
>
>
> <P034101 Letter Granting Request For Nonpublic Info and Documents Re Tiversa To Chairman Issa.pdf>

Kelly, Andrea

From: Teleky, Kathleen <Kathleen.Teleky@mail.house.gov>
Sent: Monday, July 21, 2014 5:16 PM
To: Vandecar, Kim
Subject: RE: FTC letter authorizing non-public information to Chairman Issa

Follow Up Flag: Follow up
Flag Status: Flagged

Thank you!

From: Vandecar, Kim [<mailto:KVANDECAR@ftc.gov>]
Sent: Monday, July 21, 2014 5:10 PM
To: Barblan, Jennifer; Teleky, Kathleen; Marin, Mark; Berroya, Meghan; Lessley, Lucinda; Reavis, Brandon; Grimm, Tyler
Cc: Bumpus, Jeanne; Smith, Matthew
Subject: FW: FTC letter authorizing non-public information to Chairman Issa

Correcting Jennifer and Kathleen's addresses.

From: Vandecar, Kim
Sent: Monday, July 21, 2014 5:04 PM
To: Marin, Mark (Mark.Marin@mail.house.gov); 'jennifer.balban@mail.house.gov'; 'meghan.berroya@mail.house.gov'; 'lucinda.lessley@mail.house.gov'; 'brandon.reavis@mail.house.gov'; 'kathleen.peleky@mail.house.gov'; 'tyler.grimm@mail.house.gov'
Cc: Bumpus, Jeanne; Smith, Matthew
Subject: FTC letter authorizing non-public information to Chairman Issa

Attached please find the Commission letter authorizing the release of non-public information. Staff at the FTC is working hard to finalize the document transfer. We believe we will have this done no later than 6:00 pm today.

Please let me know if you have any questions.

Best,

Kim

RX624

Kelly, Andrea

From: Marin, Mark <Mark.Marin@mail.house.gov>
Sent: Wednesday, July 23, 2014 6:13 PM
To: Bumpus, Jeanne
Cc: Barblan, Jennifer; Grimm, Tyler; Berroya, Meghan; Reavis, Brandon; Lessley, Lucinda; Vandecar, Kim
Subject: Re: Meeting with FTC staff

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Red Category

Thanks Jeanne - please let us look at our calendars and get right back to you. Many thanks - Mark

On Jul 23, 2014, at 4:52 PM, "Bumpus, Jeanne" <JBumpus@ftc.gov> wrote:

Mark, Jenn, and Tyler,

We wanted to get back to you regarding scheduling. . . We'd like first to bring up senior Commission staff as well as staff working on the LabMD case, including Alain Sheer, to meet with you before scheduling interviews. . . Would you be able to do this in the earlier part of next week? Wednesday is preferable on our end. . . If next week doesn't work, we're also available the week of August 11. . . If we're unable to answer your questions at the meeting, Alain Sheer would be available for an interview starting in mid-August, and we're checking with Ruth Yodaiken on her August schedule. Thank you,

Jeanne Bumpus
Office of Congressional Relations
Federal Trade Commission
326-2946

RX626

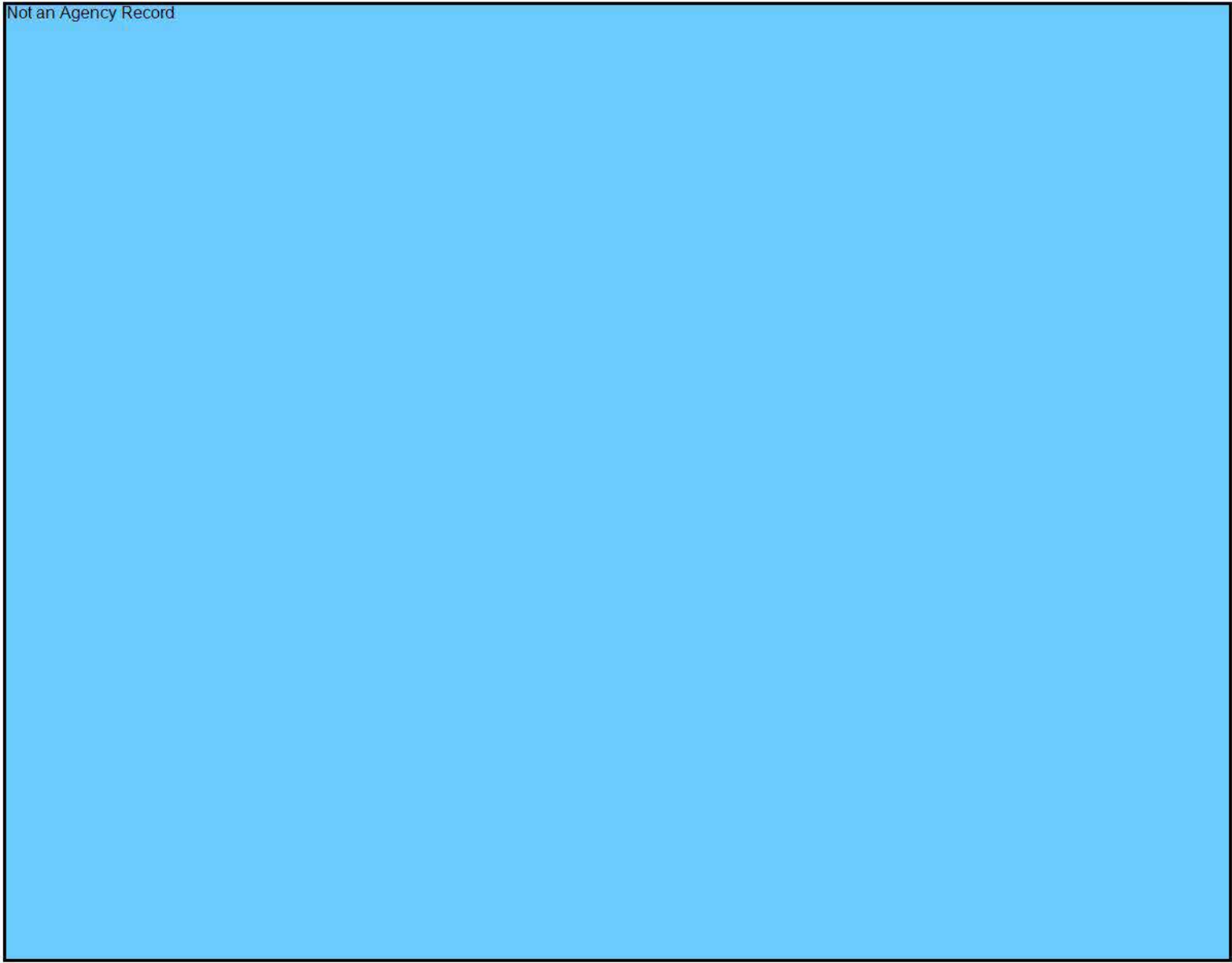
Kelly, Andrea

From: Satalin, Patrick <Patrick.Satalin@mail.house.gov>
Sent: Wednesday, July 23, 2014 10:31 AM
To: Burstein, Aaron
Subject: Not an Agency Record

Attachments:

Hey Aaron,
I hope you are doing well. The FTC is going to be getting attacked at the OGR Committee tomorrow (Peter sits on this Committee). If you have a few minutes, would love to chat with you about this today to see if there is anything we could raise that would be helpful for you all. Let me know. Thanks Aaron.

Patrick



RX627



From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Friday, July 18, 2014 12:28 PM
To: Simons, Claudia A.
Cc: Grimm, Tyler <Tyler.Grimm@mail.house.gov>
Subject: Letter from Chairman Issa

Claudia –

Attached please find a letter from Chairman Issa. Please confirm receipt at your earliest convenience.

Please feel free to call with any questions.

Thanks,
Jen

Jennifer Barblan
Senior Counsel
Committee on Oversight and Government Reform
Rep. Darrell E. Issa, Chairman
(202) 225-5074
Jennifer.Barblan@mail.house.gov

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DeJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DeSANTIS, FLORIDA

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

LAWRENCE J. BRADY
STAFF DIRECTOR

July 18, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Madam Chairwoman:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company the Federal Trade Commission relied upon as a source of information in investigations and enforcement actions. The Committee has learned that the FTC received information on nearly 100 companies from Tiversa, and initiated investigations or enforcement actions against multiple companies after receiving the information. The Committee has received serious allegations against Tiversa related to the ways that the company collected and used that information. In the course of investigating those allegations, the Committee obtained documents and testimony that show the company's business practices cast doubt on the reliability of the information that Tiversa supplied to the FTC. Given what the Committee has learned so far, I have serious reservations about the FTC's reliance on Tiversa as a source of information used in FTC enforcement actions. I am also concerned that the FTC appears to have acted on information provided by Tiversa without verifying it in any meaningful way.

From the information the Committee has gathered the relationship between the FTC and Tiversa dates back to 2007. In July 2007, Tiversa and the FTC testified before the Oversight and Government Reform Committee about the dangers of peer-to-peer networks.¹ Following Tiversa's July 2007 testimony, the FTC had a number of conversations with Tiversa about the risks of inadvertent sharing on peer-to-peer networks.² According to documents obtained by the Committee, after at least two telephone conversations between FTC and Tiversa employees,

¹ H. Comm. on Oversight & Gov't Reform, *Hearing on Inadvertent File Sharing Over Peer-to-Peer Networks*, 110th Cong. (July 24, 2007) (H. Rept. 110-39).

² E-mail traffic indicates that representatives from the FTC and Tiversa held a conference call with an online meeting component on October 26. E-mail from [FTC Employee 1], Fed. Trade Comm'n, to Robert Boback, CEO, Tiversa, Inc. (Oct. 22, 2007 2:23 p.m.) ("We'll plan on speaking with you at 10:30 on Friday morning (10/26). I'll check on our ability to do the call with web access to be able to view a presentation." E-mail from Robert Boback, CEO, Tiversa, Inc., to [FTC Employee 1], Fed. Trade Comm'n (Oct. 22, 2007 3:25 p.m.) ("I have scheduled our demonstration for Friday at 10:30."). Another phone conversation appears to have occurred on December 19, 2007. E-mail from Robert Boback, CEO, Tiversa, Inc., to [FTC Employee 1], Fed. Trade Comm'n (Dec. 11, 2007 2:04 p.m.) ("2 pm on Wednesday (12/19) will work. Let's plan for that time.").

The Honorable Edith Ramirez
 July 18, 2014
 Page 2

Robert Boback, Tiversa's CEO, sent information to the FTC in December 2007.³ It is unclear what specific information Tiversa sent to the FTC at that time or how that information was used.

In 2009, Tiversa and FTC again testified before the Oversight and Government Reform Committee at another hearing on the risk of inadvertent sharing on peer-to-peer networks.⁴ The Committee has learned that around the same time as this hearing, the FTC contacted Tiversa and asked for information about companies with large data breaches.⁵ In order to receive the information, the FTC issued a civil investigative demand to the Privacy Institute, an entity Tiversa apparently created for the specific and sole purpose of providing information to the FTC. Mr. Boback explained the relationship between Tiversa and the Privacy Institute during a transcribed interview with the Committee. He testified that Tiversa lawyers set up the Privacy Institute "to provide some separation from Tiversa from getting a civil investigative demand at Tiversa, primarily. And, secondarily, it was going to be used as a nonprofit, potentially, but it never did manifest."⁶

Through the Privacy Institute, Tiversa produced a spreadsheet to the FTC that contained information on data breaches at a large number of companies.⁷ Mr. Boback further testified that Tiversa provided information on "roughly 100 companies" to the FTC.⁸

In February 2010, the FTC announced that it notified "almost 100 organizations" that personal information had been shared from the organizations' computer networks and was available on peer-to-peer networks.⁹ The FTC also announced that it opened non-public investigations concerning an undisclosed number of companies.¹⁰ The timing of the Privacy Institute's production of negative information on "roughly 100 companies" to the FTC, and the FTC's subsequent announcement that it notified "almost 100 organizations" that they were under FTC scrutiny, creates the appearance that the FTC relied substantially on the information that Tiversa collected and provided.

That same month, Mr. Boback gave an interview to *Computerworld* about the FTC's announcement.¹¹ He stated, "We were happy to see that the FTC [has] finally started recognizing that P2P [peer-to-peer] is a main source for criminals to gain access to consumer's personally identifiable information for ID theft and fraud."¹² Mr. Boback also stated that 14 of the companies the FTC contacted had already reached out to Tiversa for assistance, and that 12

³ E-mail from Robert Boback, CEO, Tiversa, Inc., to [FTC Employee 1], Fed. Trade Comm'n (Dec. 19, 2007 3:08 p.m.) ("Per our discussion...see attached.").

⁴ H. Comm. on Oversight & Gov't Reform, *Hearing on Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security*, 111th Cong. (July 29, 2009) (111-25).

⁵ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback, CEO, Tiversa, Inc., at 169 (June 5, 2014) [hereinafter Boback Tr.].

⁶ Boback Tr. at 42-43.

⁷ Boback Tr. at 169.

⁸ Boback Tr. at 171.

⁹ Fed. Trade Comm'n, Press Release, *Widespread Data Breaches Uncovered by FTC Probe* (Feb. 22, 2010).

¹⁰ *Id.*

¹¹ Jaikumar Vijayan, *FTC seeks extensive information from firms being investigated for P2P breaches*, COMPUTERWORLD, Feb. 25, 2010,

http://www.computerworld.com/s/article/9162560/FTC_seeks_extensive_information_from_firms_being_investigat_ed_for_P2P_breaches?taxonomyId=84&pageNumber=1.

¹² *Id.*

The Honorable Edith Ramirez
July 18, 2014
Page 3

of those companies received civil investigative demands.¹³ Because Tiversa was benefiting commercially from the fact that the FTC was investigating the companies that Tiversa itself referred to the FTC, it is critical for the Committee to understand the relationship between the FTC and Tiversa, and whether Tiversa manipulated the FTC in order to enrich themselves.

In order to assist the Committee in its investigation, please provide the following documents as soon as possible, but by no later than 5:00 p.m. on July 21, 2014:

1. All civil investigative demand letters the FTC sent to the Privacy Institute and Tiversa, Inc.
2. All documents, including spreadsheets, produced by the Privacy Institute or Tiversa to the FTC in response to any civil investigative demand letters sent by the FTC.
3. All letters or other notices sent by the FTC sent to “almost 100 organizations” as discussed in a February 22, 2010, FTC press release.
4. All civil investigative demand letters the FTC sent as part of the investigations announced in the February 22, 2010, FTC press release.

The Committee on Oversight and Government Reform is the principal investigative committee of the U.S. House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate “any matter” at “any time.” An attachment to this letter provides additional information about responding to the Committee’s request.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Tyler Grimm or Jennifer Barblan of the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,



Darrell Issa
Chairman

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

¹³ *Id.*

ONE HUNDRED THIRTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

Phone: (202) 225-5331
Fax: (202) 225-5851

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,

CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD, INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.
7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been

located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.

17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.
19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Schedule Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.
5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.

RX628

Kelly, Andrea

From: Smith, Matthew
Sent: Monday, July 21, 2014 6:38 PM
To: jennifer.barblan@mail.house.gov; kathleen.teleky@mail.house.gov;
Mark.Marin@mail.house.gov; megan.berroya@mail.house.gov;
lucinda.lessley@mail.house.gov; brandon.reavis@mail.house.gov;
tyler.grimm@mail.house.gov
Cc: Bumpus, Jeanne; Vandecar, Kim
Subject: Nonpublic Info and Documents Re Tiversa To Chairman Issa

Follow Up Flag: Follow up
Flag Status: Flagged

You have received 1 secure file from msmith4@ftc.gov.

Use the secure link below to download.

Dear Committee Staff,

Below you will find a link to download documents Chairman Issa requested in a letter to the FTC on July 18, 2014. As discussed with Commission staff, the information contained in these documents is highly sensitive. The link to download these documents will be active for a period of 48 hours or about 2 days. Should you have any questions, please do not hesitate to contact Kim Vandecar at (202) 326-2858.

Kind Regards,

Matt Smith

Matthew Smith
Division of Privacy and Identity Protection
Federal Trade Commission
400 7th Street, SW
Washington, D.C. 20024
Mail Stop CC-8232
Direct: (202)326-2693
Fax: (202)326-3062
Email: msmith4@ftc.gov

This email message and any attachments are confidential and may be privileged. If you are not the intended recipient, please delete the email and notify the sender.

Secure File Downloads:

Available until: **25 July 2014**

Click link to download:

[20140721final.zip](#)
708,171.51 KB

You have received attachment link(s) within this email sent via the FTC Secure Mail system. To retrieve the attachment(s), please click on the link(s).

CATEGORY 4

**Internal FTC emails and communications
regarding OGR's December 1, 2014 letter to
Commissioner Ramirez**

RX630

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DESANTIS, FLORIDA

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

LAWRENCE J. BRADY
STAFF DIRECTOR

December 1, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Ms. Ramirez:

The Committee on Oversight and Government Reform has been investigating the activities of Tiversa, Inc., a Pittsburgh-based company that purportedly provides peer-to-peer intelligence services. The Federal Trade Commission has relied on Tiversa as a source of information in its enforcement action against LabMD, Inc., a Georgia-based medical testing laboratory. The Committee has obtained documents and information indicating Tiversa failed to provide full and complete information about work it performed regarding the inadvertent leak of LabMD data on peer-to-peer computer networks. In fact, it appears that, in responding to an FTC subpoena issued on September 30, 2013, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

Despite a broad subpoena request, Tiversa provided only summary information to the FTC about its knowledge of the source and spread of the LabMD file.

Initially, Tiversa, through an entity known as the Privacy Institute, provided the FTC with information about peer-to-peer data leaks at nearly 100 companies, including LabMD.¹ Tiversa created the Privacy Institute for the specific purpose of providing information to the FTC. Despite Tiversa's claims that it is a trusted government partner, it did not want to disclose that it provided information to the FTC.²

After the FTC filed a complaint against LabMD, the agency served Tiversa with a subpoena for documents related to the matter. Among other categories of documents, the subpoena requested "all documents related to LabMD."³ In a transcribed interview, Alain Sheer,

¹ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback, Chief Executive Officer, Tiversa, Inc., Transcript at 42 (June 5, 2014) [hereinafter Boback Tr.].

² See Tiversa, Industry Outlook, Government/Law Enforcement, available at <http://tiversa.com/explore/industry/gov> (last visited Nov. 21, 2014); Boback Tr. at 42-43.

³ Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC Subpoena].

an attorney with the FTC's Bureau of Consumer Protection, told the Committee that the FTC did not narrow the subpoena for Tiversa. Sheer stated:

Q This is the specifications requested of Tiversa. No. 4 requests all documents related to LabMD. Do you know if Tiversa produced all documents related to LabMD?

A I am not sure what your question is.

Q Let me ask it a different way. Was the subpoena narrowed in any way for Tiversa?

A Not that I am aware of.⁴

In total, Tiversa produced 8,669 pages of documents in response to the FTC's subpoena. Notably, the production contained five copies of the 1,718-page LabMD Insurance Aging file that Tiversa claimed to have found on peer-to-peer networks and only 79 pages of other materials, none of which materially substantiated Tiversa's claims about the discovery of the file.

The information Tiversa gave the FTC included the IP address from which Tiversa CEO Robert Boback has claimed the company first downloaded the LabMD file, as well as other IP addresses that Tiversa claims also downloaded the file. The origin of the IP address from which Tiversa first downloaded the LabMD file was in dispute in other litigation between LabMD and Tiversa. On numerous occasions, including before the FTC, Boback maintained that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. Boback stated:

Q What is the significance of the IP address, which is 68.107.85.250?

A That would be the IP address that we downloaded the file from, I believe.

Q Going back to CX 21. Is this the initial disclosure source?

A If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.

Q When did Tiversa download [the LabMD file]?

A I believe it was in February of 2008.⁵

⁴ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer, Fed. Trade Comm'n, Transcript at 147 (Oct. 9, 2014).

⁵ In the matter of LabMD, Inc., Deposition of Robert J. Boback, CEO, Tiversa, transcript at 24-25 (Nov. 21, 2013) [hereinafter Boback Nov. 2013 FTC Tr.].

Boback also testified that Tiversa performed an investigation into the LabMD file at the request of a client.⁶ In the course of this investigation, Tiversa concluded that an IP address in Atlanta, Georgia, where LabMD was headquartered, was the initial disclosure source of the document. Boback stated:

Q There is an IP address on the right-hand side, it is 64.190.82.42. What is that?

A That, if I recall, is an IP address that resolves to Atlanta, Georgia.

Q Is that the initial disclosure source?

A We believe that it is the initial disclosure source, yes.

Q And what is that based on?

A The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.

* * *

Q So, I think you are telling me that chronologically this was the first other location for that file in juxtaposition of when you found the file at 68.107.85.250?

A We know that the file in early February, prior to this February 25 date, was downloaded from the 68.107.85.250. Upon a search to determine other locations of the file across the network, it appears that on 2/25/2008 we had a hash match search at 64.190.82.42, which resolved to Atlanta, which led us to believe that without further investigation, that this is most likely the initial disclosing source.

Q What other information do you have about 64.190.82.42?

A I have no other information. I never downloaded the file from them. They only responded to the hash match.⁷

Boback's testimony before the FTC in November 2013 made clear that Tiversa first downloaded the LabMD file from an IP address in San Diego, California, in February 2008, that it only identified LabMD as the disclosing source after performing an investigation requested by a client, and that it never downloaded the file from LabMD.

⁶ Boback Nov. 2013 FTC Tr. at 72-73 ("In 2008, when working for another client, we were attempting to identify the original disclosure source of the file that we discovered from 1 the San Diego IP address.").

⁷ Boback Nov. 2013 FTC Tr. at 41.

Tiversa withheld responsive documents from the FTC, despite the issuance of the September 2013 subpoena. These documents contradict the account Boback provided to the FTC.

On June 3, 2014, the Committee issued a subpoena to Tiversa requesting, among other information, “[a]ll documents and communications referring or relating to LabMD, Inc.”⁸ This request was very similar to the FTC’s request for “all documents related to LabMD.”⁹ Despite nearly identical requests from the FTC and the Committee to Tiversa, Tiversa produced numerous documents to the Committee that it does not appear to have produced to the FTC. Information contained in the documents Tiversa apparently withheld contradicts documents and testimony Tiversa did provide to the FTC.

An internal Tiversa document entitled “Incident Record Form,” dated April 18, 2008, appears to be the earliest reference to the LabMD file in Tiversa’s production to the Committee.¹⁰ This document states that on April 18, 2008, Tiversa detected a file “disclosed by what appears to be a potential provider of services for CIGNA.”¹¹ The Incident Record described the document as a “single Portable Document Format (PDF) that contain[ed] sensitive data on over 8,300 patients,” and explained that “[a]fter reviewing the IP address, resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.”¹² The name of the file was “insuranceaging_6.05.071.pdf,” which is the same name as the file in question in the FTC proceeding. According to the Incident Record, the IP address disclosing the file was 64.190.82.42—later confirmed to be a LabMD IP address.¹³ Upon learning about the file, CIGNA, a Tiversa client, “asked Tiversa to perform Forensic Investigation activities” on the insurance aging file to determine the extent of proliferation of the file over peer-to-peer networks.¹⁴

An August 2008 Forensic Investigation Report provided the analysis CIGNA requested. This report identified IP address 64.190.82.42—the Atlanta IP address—as proliferation point zero, and the “original source” of the Incident Record Form.¹⁵ A spread analysis included in the August 2008 forensic report stated that the file had been “observed by Tiversa at additional IP addresses” but made clear that Tiversa had not downloaded the file from either additional source because of “network constraint and/or user behavior.”¹⁶ Thus, according to this report, Tiversa had only downloaded the LabMD file from one source in Atlanta, Georgia by August 2008. This contradicts Boback’s testimony that Tiversa first downloaded the LabMD file from an IP address

⁸ H. Comm. on Oversight & Gov’t Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014).

⁹ Tiversa FTC Subpoena.

¹⁰ Tiversa Incident Record Form, ID # CIG00081 (Apr. 18, 2008).

¹¹ *Id.*

¹² *Id.* (emphasis added).

¹³ *Id.*

¹⁴ Tiversa, Forensic Investigation Report for Ticket #CIG00081 (Aug. 12, 2008). This letter uses the phrase “forensic report” to describe this and a second report created by Tiversa about the LabMD file because that is the title used by Tiversa. It is not clear what, if any, forensic capabilities Tiversa possesses.

¹⁵ *Id.*

¹⁶ *Id.*

The Honorable Edith Ramirez

December 1, 2014

Page 5

in San Diego, California. If Tiversa had in fact downloaded the LabMD file from a San Diego IP address in February 2008, then that fact should be included in this 2008 forensic report. It is not.

One of the two additional IP addresses is located in San Diego, California. It is a different IP address, however, than the one from which Tiversa claims to have originally downloaded the file.¹⁷ Further, Tiversa did not observe that this San Diego IP address possessed the LabMD file until August 5, 2008.¹⁸ Thus, according to this report, Tiversa did not observe any San Diego IP address in possession of the LabMD file until August 2008. Again, the report stands in stark contrast to Boback's testimony that Tiversa first downloaded the LabMD file from a different San Diego IP address in February 2008.

In addition, both the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report stated that the LabMD file was "detected being disclosed" in April 2008. Neither report indicated that Tiversa first downloaded the file from the San Diego IP address—an IP address not listed on either report—on February 5, 2008. Boback's deposition testimony and a cursory four-line document marked as exhibit CX-19 seem to be the only evidence that Tiversa first downloaded the LabMD file from a San Diego IP address in February 2008.

These documents contradict the information Tiversa provided to the FTC about the source and spread of the LabMD file. If Tiversa had, in fact, downloaded the LabMD file from the San Diego IP address and not from the Georgia IP address, then these reports should indicate as such. Instead, the San Diego IP address is nowhere to be found, and the Georgia IP address appears as the initial disclosing source on both reports.

Tiversa also produced an e-mail indicating that it originally downloaded the LabMD file from Georgia – and not from San Diego as it has steadfastly maintained to the FTC and this Committee. On September 5, 2013, Boback e-mailed Dan Kopchak and Molly Trunzo, both Tiversa employees, with a detailed summary of Tiversa's involvement with LabMD. Why Boback drafted the e-mail is unclear. He wrote, "[i]n 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."¹⁹

As noted above, according to Alain Sheer, a senior FTC attorney assigned to the LabMD matter, the FTC did not narrow the September 2013 subpoena requiring Tiversa to produce, among other documents, "all documents related to LabMD."²⁰ Tiversa withheld these relevant

¹⁷ The IP address reported on the August 2008 forensic report that resolves to San Diego, California is 68.8.250.203. Boback testified, however, that Tiversa first downloaded the LabMD file from IP address 68.107.85.250 on February 5, 2008. Tiversa concluded in the report that the second IP address on which it observed the file was "most likely an IP shift from the original disclosing source."

¹⁸ *Id.*

¹⁹ E-mail from Robert Boback, CEO, Tiversa, to Dan Kopchak & Molly Trunzo (Sept. 5, 2013) (emphasis added) [TIVERSA-OGR-0028866-67].

²⁰ Tiversa FTC Subpoena.

The Honorable Edith Ramirez

December 1, 2014

Page 6

documents about its discovery and early forensic analysis of the LabMD file from the FTC. These documents directly contradict testimony that Boback provided to the FTC, and call Tiversa's credibility into question. Boback has not adequately explained why his company withheld documents, and why his testimony is not consistent with reports Tiversa created at the time it discovered the LabMD file.

It is unlikely that the LabMD file analyzed in the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report is different from the so-called "1718 file" at issue in the FTC proceeding, particularly given Boback's testimony to the FTC about how Tiversa's system names files.²¹ If, however, the earlier reports do refer to a different file, then Tiversa neglected to inform the FTC of a second, similarly sized leak of LabMD patient information.

Tiversa's June 2014 forensic report is the only report provided to this Committee that substantiates Boback's claims.

Tiversa produced to the Committee a forensic report on the LabMD file that it created in June 2014. Tiversa created this report and others related to testimony previously provided to the Committee after the investigation began. While outside the scope of the FTC's subpoena due to the date of the document, this is the only report supporting Tiversa's claim that it first downloaded the file from the San Diego IP address. This report contradicts information Tiversa provided to CIGNA in the April 2008 Incident Record Form and August 2008 Forensic Investigative Report—documents created much closer to when Tiversa purportedly discovered the LabMD document on a peer-to-peer network. The fact that Tiversa created the only forensic report substantiating its version of events after the Committee began its investigation raises serious questions.

This most recent report states that Tiversa's systems first detected the file on February 5, 2008, from a San Diego IP address (68.107.85.250) not included in either of the 2008 documents. According to the spread analysis, this San Diego IP shared the file from February 5, 2008, until September 20, 2011. Yet, despite allegedly being downloaded before both the April or August 2008 reports, neither 2008 document mentions that Tiversa downloaded this document.

The June 2014 report also states that the LabMD IP address (64.190.82.42) shared the file between March 7, 2007, and February 25, 2008. Thus, according to this report, by the time Tiversa submitted an Incident Record Form to CIGNA in April 2008, the LabMD IP address was no longer sharing the file. Furthermore, the report does not describe why Tiversa's system did not download the file from the Georgia IP address, even though the technology should have downloaded a file that hit on a search term, in this case "CIGNA," each time a different computer shared the document. The June 2014 report includes no reference to the other San Diego IP address discussed in the August 2008 forensic report as being in possession of the LabMD file.

²¹ Boback Nov. 2013 FTC Tr. at 40-41 (describing that a file's "hash" or title identifies "exactly what that file is." The title of the LabMD document described in the April and August 2008 documents is the same as the title of the document in the FTC proceeding).

Tiversa did not make a full and complete production of documents to this Committee. It is likely that Tiversa withheld additional documents from both this Committee and the FTC.

On October 14, 2014, Tiversa submitted a Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity.²² Chief Administrative Law Judge D. Michael Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose."²³ Tiversa included two e-mails from 2012 as exhibits to the Notice of Information. According to Tiversa, these e-mails demonstrate that Wallace could not have fabricated the IP addresses in question in October 2013, because he previously included many of them in e-mails to himself and Boback a year prior.²⁴

Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission in the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. In its Notice of Information, Tiversa did not explain how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information and do not explain what exactly Wallace conveyed to Boback in November 2012 or why he conveyed it.

If Boback did in fact receive this information in November 2012, his June 2013 deposition testimony is questionable. It is surprising that Tiversa would have supplied inaccurate information to the FTC when Boback himself apparently received different information just months prior. Tiversa should have located and produced these e-mails pursuant to the September 2013 subpoena, and it should have been available for Boback's June 2013 deposition.

Tiversa's failure to produce numerous relevant documents to the Commission demonstrates a lack of good faith in the manner in which the company has responded to subpoenas from both the FTC and the Committee. It also calls into question Tiversa's credibility as a source of information for the FTC. The fact remains that withheld documents contemporaneous with Tiversa's discovery of the LabMD file directly contradict the testimony and documents Tiversa did provide. In the Committee's estimation, the FTC should no longer consider Tiversa to be a cooperating witness. Should the FTC request any further documents from Tiversa, the Commission should take all possible steps to ensure that Tiversa does not withhold additional documents relevant to the proceeding.

²² Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request For Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014), <http://www.ftc.gov/system/files/documents/cases/572572.pdf> [hereinafter Notice of Information].

²³ *LabMD Case: FTC gets green light to grant former Tiversa employee immunity in data security case*, PHIprivacy.net, Nov. 19, 2014, <http://www.phiprivacy.net/labmd-case-ftc-gets-green-light-to-grant-former-tiversa-employee-immunity-in-data-security-case/>.

²⁴ Notice of Information at 4.

The Honorable Edith Ramirez

December 1, 2014

Page 8

I have enclosed the documents discussed herein with this letter, so that your staff may examine them. All documents are provided in the same form in which Tiversa produced them to the Committee.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X. If you have any questions, please contact the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,



Darrell Issa
Chairman

Enclosures

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

Ms. Kelly Tshibaka, Acting Inspector General, U.S. Federal Trade Commission

Ms. Laura Riposo VanDruff, Complaint Counsel, U.S. Federal Trade Commission



INVESTIGATION REQUEST FORM

Section 1 Customer Information	
Organization Name	CIGNA
Contact Name	Sean Ryan
Contact Phone Number	(860) 226-7107
Contact Email Address	sean.ryan@cigna.com

Section 2 Incident Information	
Tiversa Incident Number	CIG00081
Date of Incident	4/18/2008

Section 3 Requested Forensic Services	
<p>File Disclosure Investigation</p> <input type="checkbox"/> 1. Disclosure Source Identification <input type="checkbox"/> 2. Disclosure Source Geo-location <input type="checkbox"/> 3. Identify Additional Disclosure Source Files <input type="checkbox"/> 4. File Proliferation Assessment <input type="checkbox"/> 5. Proliferation Point Identification <input type="checkbox"/> 6. Proliferation Point Geo-location <input type="checkbox"/> 7. Proliferation Point Associated Files	<p>Search Investigation</p> <input type="checkbox"/> 12. Review Stored Searches For File Targeting <input type="checkbox"/> 13. Track Searches for Specific File or Term
<p>Persons of Interest (PoI)</p> <input type="checkbox"/> 8. Identify Persons of Interest <input type="checkbox"/> 9. Track Specific Behavior of Persons of Interest <input type="checkbox"/> 10. Identify Files Associated with Persons of Interest <input type="checkbox"/> 11. Track Persons of Interest Download Behavior	<p>Miscellaneous</p> <input type="checkbox"/> 14. Prosecution Support (Complete Section 4) <input type="checkbox"/> 15. Other (Complete Section 4)

Section 4 Specific Information Related to Request

TIVERSA – CUSTOMER RESTRICTED

LABMD - SUPP. PROD.

0693

4/30/15



INCIDENT RECORD FORM

Section 1 Customer Information	
Organization Name	CIGNA
Contact Name	Sean Ryan
Contact Phone Number	(860) 226-7107
Contact Email Address	sean.ryan@cigna.com

Section 2 Incident Information	
Tiversa Incident Number	CIG00081
Related Tiversa Incident Numbers	None
Date of Incident	4/18/2008
Severity	Urgent

Section 3 Disclosure Information	
IP Address	64.190.82.42
Disclosure Type	Partner / Provider
Summary Disclosure Name/ID	LAB MD
Filenames	[64.190.82.42]insuranceaging_6.05.071.pdf

Section 4 Incident Summary

On 4/18/2008, 1 file was detected being disclosed by what appears to be a potential provider of services for CIGNA.

The information appears to be a single Portable Document Format (PDF) file that contains sensitive data on over 8,300 patients. Some of the information includes: Patients Full Name, SSN, DOB, Insurance Policy Numbers, Patient Diagnostic Codes, and other information. Of the 8,342 patient records, at least 113 appear to be listed as insured by CIGNA.

After reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.

TIVERSA – CUSTOMER RESTRICTED

LABMD - SUPP. PROD.

0694

Section 5 Additional Questions That Tiversa Can Address

More information can be gathered related to this disclosure by leveraging Tiversa’s P2P File Sharing Forensic Investigation Services. If requested, please fill out the Investigation Request form located below and submit to your Account Manager.

Who is the individual disclosing the information?

Select investigation services #1 and #3

What else is this individual sharing or disclosing?

Select investigation service #3

Where is this individual located in the world?

Select investigation service #2

Did the files spread to other users of the network?

Select investigation services #4

TIVERSA – CUSTOMER RESTRICTED

LABMD - SUPP. PROD.

0695

4/30/15



Forensic Investigation Report for Ticket #CIG00081

August 12, 2008

CONFIDENTIAL

LABMD - SUPP. PROD.

0696

4/30/15

1. Introduction

Tiversa monitors peer-to-peer file sharing networks (P2P) for CIGNA 24/7/365 to identify disclosed sensitive or confidential CIGNA-related information and to record P2P users searching for this information. For each file disclosure, Tiversa provides a disclosure ticket to CIGNA. Each ticket includes the name of the file(s) disclosed, IP on which the files were obtained, the likely source of the disclosure, and copies of the disclosed files. In some cases, more information is required in order to decide what actions to take or to determine if remedial actions have worked. In these instances, Forensic Investigation Services are required.

This Forensic Investigation Report (FIR) summarizes the results and suggested actions of Tiversa's Forensic Investigation Services for Ticket CIG00081, as requested by CIGNA.

1.1 Ticket CIG00081 Summary

The specifics of this ticket as reported were as follows:

- Date Submitted: 4/18/2008
- Disclosing IP Location: 64.190.82.42
- Number of Files Disclosed: 1 CIGNA file (19 total files)
- Probable Disclosure Source: Partner/Provider
- Probable Disclosure Name/ID: Lab MD
- Severity: Urgent

Ticket Write-up Copy:

On 4/18/2008, 1 file was detected being disclosed by what appears to be a potential provider of services for CIGNA.

The information appears to be a single Portable Document Format (PDF) file that contains sensitive data on over 8,300 patients. Some of the information includes: Patients Full Name, SSN, DOB, Insurance Policy Numbers, Patient Diagnostic Codes, and other information. Of the 8,342 patient records, at least 113 appear to be listed as insured by CIGNA.

After reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.

CIGNA asked Tiversa to perform Forensic Investigation activities related to the above ticket in order to ascertain if any of the disclosed files have proliferated across the P2P.

2. Investigation Findings

2.1 File Proliferation Analysis

The CIGNA-related file identified in Ticket #81, as well as some of the files not related to CIGNA, have been observed by Tiversa at additional IP addresses on the P2P. However, network constraints and/or user behavior prevented Tiversa from downloading the files from these additional sources. Most likely, the user logged off the P2P prior to or while Tiversa was attempting to acquire the files.

Regardless, information regarding these new observations is included in Figure 2-1-1 immediately below.

**Figure 2-1-1:
File Proliferation Details**

Proliferation Point	File Title	IP Address	Date Observed	IP Geo-Location	ISP	Source
0	insuranceaging_6.05.071.pdf	64.190.82.42	4/18/08	Atlanta, GA	Cypress Communications	Original Source from Ticket #81
1	insuranceaging_6.05.071.pdf	64.190.79.36	8/1/08	Oakwood, GA	Cypress Communications	Probably an IP shift of original source
2	insuranceaging_6.05.071.pdf	68.8.250.203	8/5/08	San Diego, CA	Cox Communications	Unknown (based on other files observed, possible Information Concentrator)

Based on the other files available at the new IP addresses, Proliferation Point #1 (from Figure 2-1-1 above) is most likely an IP shift from the original disclosing source identified in Ticket #81. However, the other files present at Proliferation Point #2 suggest that this source could be an Information Concentrator. Because Tiversa analysts were only able to visually observe these new sources, rather than actually download files, further data collection and analysis may be required for full source identification of the proliferation points.

2.2 Additional Data Collection/ Analysis

Tiversa is currently attempting to re-acquire these sources and download any relevant files from them.

3. Conclusions/ Suggested Actions

It appears evident that the files from Ticket #81 have proliferated across the P2P and are available from additional IP addresses. However, clear identification of these new sources is not conclusive at this time. Tiversa will update this report as new information becomes available.

In the meantime, CIGNA and/or LabMD investigations of the data currently available could be executed. If additional data from Tiversa is required, it can be provided -- for instance, a full listing of files disclosed from the original source (even if those files are not related to CIGNA) can be made available.



2000 Corporate Drive, Suite 300
Wexford, Pennsylvania 15090

724 940-9030
724 940-9033

www.tiversa.com

**LABMD - SUPP. PROD.
0700**

From: Robert Boback <rboback@tiversa.com>
Sent: Thursday, September 5, 2013 3:20 PM
To: Dan Kopchak <dkopchak@tiversa.com>; Molly Trunzo <mtrunzo@tiversa.com>
Subject: Tiversa

I wanted to provide updated information regarding the question of litigation involving Tiversa. During our call, I discussed litigation in which Tiversa is a plaintiff against our former patent firm. That is still ongoing. Earlier in 2013, Tiversa was also engaged in a separate litigation with a company called LabMD, which is based in Georgia. Tiversa, Dartmouth College and Professor Eric Johnson (Tuck Business School) was sued by LabMD by its CEO, Michael Daugherty as he alleged that Tiversa "hacked" his company in an effort to get a file containing nearly 9,000 patient's SSNs and medical information and provided the information to Dartmouth and Eric Johnson for a DHS-funded research project. Mr. Daugherty has little to no understanding of P2P or Information security which is what caused him to think that he was "hacked" and which resulted in his widespread government conspiracy theory that followed. He also suggested in the litigation that because he would not do business with Tiversa to remediate the problem, that Tiversa "kicked the file over to the feds [FTC]" (and Dartmouth) and the FTC sent him a questionnaire about the breach, which caused him "great harm" due to the widespread "government shakedown of small business." He claimed that Tiversa was attempting to extort money from him to "answer his questions" as a part of the larger conspiracy. The reason that I did not mention this during our discussion is that the case was dismissed due to jurisdiction (his real estate attorney friend filed it in Georgia). He subsequently appealed two times, and lost both, the final of which was ruled on in February 2013. As an interesting sidebar to this story, Mr. Daugherty began writing a book about the government overreach and his great conspiracy theory of the government war on small business. When our attorneys learned of what was coming in the book (from his blog postings about the book), we quickly served his counsel with a C&D as his "true story" was full of inaccurate statements about me and Tiversa. Unfortunately, Mr. Daugherty sees himself as "Batman" (no joke) and he chose to continue on with his book and starting scheduling speaking engagements where he would discuss his "true story" about how the government is out to "get" small business and that the FTC and Tiversa (and presumably Dartmouth) are the ring leaders. His book, "Devil inside the Beltway" is to be released later this month. While I do not expect this book to be on the NY Times best seller list, I cannot sit idly by and allow such a gross distortion of the facts and mischaracterization of Tiversa, and me, in his efforts to sell his book and create a "name" for himself on any speaking tour.

That said, Tiversa filed a complaint in federal court today citing a number of counts including but not limited to Defamation, Slander, Libel, and others against Mr. Daugherty and LabMD. Tiversa is not litigious and it was our hope that he would conduct himself appropriately after receiving the C&D in November of 2012. But again, he sees himself as Batman.

Here is the real series of events that occurred in this case:

Tiversa, as you know, downloads leaked information on behalf of clients, individual, corporate and/or federal. In the process of downloading information, we often get files that are not related to our clients but are nonetheless sensitive. We call this "dolphin in the tuna net"....for example, if we were looking for "Goldman Sachs" and our system finds a file with the term "Goldman" in it. The file may have the name "Henry Goldman" but our system just saw "Goldman" and downloaded it, in the event it related to Goldman Sachs. After the file would be downloaded, it would be reviewed by an Analyst which would determine that it was NOT related to Goldman Sachs, but it may or may not include SSNs or other sensitive information. This was the case with LabMD.

In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name "LabMD" in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable. We could have chosen to do nothing at all and pretend that we never saw the file. That approach would leave both LabMD and the 9000 victims at very high risk (and growing) of fraud and identity theft. Needless to say, we contacted the company to inform them of the file with their company name on it. After providing the file with all of the information that we had, the Mr. Daugherty asked us for additional information that we did not have. We told him that we could perform the services but it would take a few weeks and would cost about \$15K. After hearing this, he asked us to send him the SOW for the services. 3 weeks after providing the SOW and not hearing anything in return, I reached out to Mr. Daugherty to see if he had any questions (re: SOW) and he told me never to contact him again with no further explanation. We did not.

Tuck Business School at Dartmouth (and Professor Eric Johnson) used Tiversa in early 2006 for a research project to determine to what extent, if any, leaked financial documents were able to be found on P2P networks. The research consisted of Dartmouth providing simple and straightforward search terms to Tiversa like "bank" and "account" to locate and download files using Tiversa's engine to a hard drive that Dartmouth owned and controlled. Tiversa only issued the searches but was not able to see the actual downloads. The downloads were stored on a hard drive that graduate students at Dartmouth were to later evaluate. Although Dartmouth was researching this using resources from a grant by DHS, Tiversa was not paid anything for our participation. The research was impactful and resulted in a number of articles being published. With the prior success of the financial research, Dartmouth wanted to followup with a second research project focused on medical information in 2008. Following the exact same procedure, the medical research was completed and widely published in early 2009. Again, Tiversa did not receive any compensation whatsoever for our part in the project. Upon reading the research paper, one of the many example files that were used to demonstrate the problem was the file in question with LabMD. Tiversa did not know that the file was included in the research as we did not see the downloads, only the search terms. Frankly, it was not surprising that the file was found because it was never addressed with LabMD therefore the file continued to spread across the P2P network.

I was called to testify before Congress twice in 2009, once in May and the second in July, as they were investigating breaches of security via P2P. At the direction of Congress, Tiversa was asked to demonstrate the extent and severity of the problem. Tiversa then provided Congress with numerous, redacted, examples of file disclosure that affected government, private and public enterprises, and individuals. Shortly after the hearings, Tiversa was visited by the FTC. The senior representatives from the FTC wanted to see the non-redacted versions of the files discussed with Congress as one of their missions is to help consumers handle ID theft. When Tiversa asked what would happen if we refused to provide the information, the FTC stated that they would issue a Civil Investigative Demand (CID) which acts as a federal subpoena to gain access to the information. We told them that they would need to do that and then we would provide the information in accordance with the subpoena. The FTC issued a subpoena that asked us to provide any file, regardless of source, that disclosed >100 SSNs. We provided over 100 files to the FTC in accordance with the federal subpoena and the LabMD file was still one of them as it remained on the P2P network. We had no insight/control as to what the FTC was going to do with the information once they received it. Tiversa was not compensated in any way for providing this information to the FTC.

Apparently, the FTC sent questionnaires to some, if not all, of the companies or organizations that breached the sensitive information. The FTC posted on its website a copy of a standard letter(s) that was sent, which is how we knew that they had sent a letter or letters. We had no further communication with the FTC regarding the breaches or their investigations.

LabMD sued Tiversa/Dartmouth/Eric Johnson. Case was dismissed (all three times) for jurisdiction issues.

LABMD - SUPP. PROD.

0701

4/30/15

RX630

Mr. Daugherty starts writing his book about his problems and blames everyone but himself and his lax security measures at LabMD. He refuses to provide any information to the FTC questionnaire saying it's a "witch hunt."

To this date, I have not heard of Mr. Daugherty spending a single penny in notification or protection of ANY of the over 9000 cancer/medical patients in which he violated their privacy and well established HIPAA laws. He sees himself as the "victim" when he is actually the perpetrator. He intends to capitalize on his "victim" status by becoming "Batman" on a crusade for all Americans against government overreach.

The FTC sued Mr. Daugherty and LabMD last week for his non-compliance with a federal subpoena (CID). In the FTC complaint, it noted that over 500 people (of the 9000 in the LabMD file) have become victims of ID theft and fraud according to a Sacramento, CA Police Department investigation. I would suppose that multiple states AG's offices could pursue litigation against LabMD and Mr. Daugherty as well for not notifying the individuals (that reside in the various states) that their information had been breached. It is a requirement in 47 of the 50 states. I also only suppose that it is matter of time before there will be a class action suit file against LabMD and Mr. Daugherty for the continued reckless breach of patient information.

Mr. Daugherty continues to hype his book, even going as far to have a cheesy trailer made about the book which is full of false statements regarding Tiversa and me. He continues to suggest that Tiversa is "government funded" which we are not, and never have been. Tiversa has only received one round of funding in 2006 by Adams Capital Management.

In my opinion, he needs to draw some connection between Tiversa, "hacking" and the government in an effort to sell his book and, more importantly, claim that he was not required to compensate the 9000 true victims of this story.

Tiversa filed a Defamation suit against LabMD and Mr. Daugherty in federal court on September 5, 2013.

Essentially, Tiversa was trying to help the 9000 people by informing LabMD that there was a problem. Unfortunately, LabMD took the "shoot/sue the messenger" approach.

LABMD - SUPP. PROD.

0702

4/30/15

Confidential - For Committee and Staff Use Only

TIVERSA_OGB_0028867

RX631

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Thursday, December 18, 2014 11:26 AM
To: OALJ
Cc: reed.rubinstein@dinsmore.com; William A. Sherman II (william.sherman@dinsmore.com); prashant.khetan@causeofaction.org
Subject: FTC Docket No. 9357 -- letter from Secretary Clark
Attachments: 2014.12.16 Letter from D. Clark to Chairman Issa.pdf

Dear Chief Administrative Law Judge Chappell:

Complaint Counsel has learned that the Secretary of the Commission, Donald Clark, transmitted the attached letter to Chairman Darrell Issa.

Respectfully Submitted,

Laura Riposo VanDruff
Complaint Counsel

Laura Riposo VanDruff
Federal Trade Commission
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W., CC-8232
Washington, DC 20580
202.326.2999 (direct)
202.326.3393 (facsimile)
lvandruff@ftc.gov



Office of the Secretary

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

December 16, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Issa:

Please know that because the matter of LabMD, Inc is still in administrative adjudication, your letter of December 1, 2014 has not been shared with the Chairwoman or the Commissioners. However, Chairwoman Ramirez has asked me to write and thank you on her behalf. Please also know, that after advising your Committee staff, the FTC's Complaint Counsel shared your letter with the Administrative Law Judge in the LabMD, Inc. matter, and with counsel for LabMD and Tiversa. Thank you again for sharing your findings.

Sincerely,

A handwritten signature in blue ink that reads "Donald S. Clark".

Donald S. Clark
Secretary of the Commission

RX632

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Tuesday, December 02, 2014 10:15 AM
To: Shonka, David C.
Cc: Bumpus, Jeanne; Vandecar, Kim; White, Christian S.; Schoshinski, Robert
Subject: In re LabMD (No. 9357) -- (b)(5)

Good morning, Dave.

(b)(5)



Best regards,

Laura

Laura Riposo VanDruff
Federal Trade Commission
Assistant Director, Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W., CC-8232
Washington, DC 20580
202.326.2999 (direct)
202.326.3393 (facsimile)
lvandruff@ftc.gov

RX634

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Tuesday, December 16, 2014 11:43 AM
To: VanDruff, Laura Riposo
Subject: FW: Response to Chairman Issa
Attachments: 14.12.16 Letter to Chairman Issa.pdf

Hi Laura,

Attached please find the response we just sent to Chairman Issa's letter of December 1.

Jeanne



Office of the Secretary

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

December 16, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Issa:

Please know that because the matter of LabMD, Inc is still in administrative adjudication, your letter of December 1, 2014 has not been shared with the Chairwoman or the Commissioners. However, Chairwoman Ramirez has asked me to write and thank you on her behalf. Please also know, that after advising your Committee staff, the FTC's Complaint Counsel shared your letter with the Administrative Law Judge in the LabMD, Inc. matter, and with counsel for LabMD and Tiversa. Thank you again for sharing your findings.

Sincerely,

A handwritten signature in blue ink that reads "Donald S. Clark".

Donald S. Clark
Secretary of the Commission

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Tuesday, December 16, 2014 11:44 AM
To: Bumpus, Jeanne
Subject: RE: Response to Chairman Issa

Thank you, Jeanne.

Laura

From: Bumpus, Jeanne
Sent: Tuesday, December 16, 2014 11:43 AM
To: VanDruff, Laura Riposo
Subject: FW: Response to Chairman Issa

Hi Laura,

Attached please find the response we just sent to Chairman Issa's letter of December 1.

Jeanne

RX635

Kelly, Andrea

From: Vandecar, Kim
Sent: Monday, December 01, 2014 1:11 PM
To: VanDruff, Laura Riposo
Cc: Bumpus, Jeanne
Subject: FW: Letter from Chairman Issa
Attachments: 2014-12-01 DEI to Ramirez-FTC - Tiversa Documents w Attachments.pdf

From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Monday, December 01, 2014 1:05 PM
To: Bumpus, Jeanne; Vandecar, Kim
Cc: Grimm, Tyler
Subject: Letter from Chairman Issa

Jeanne and Kim –

I hope you both had a nice Thanksgiving. Attached please find a letter from Chairman Issa, accompanied by documents discussed within the letter that appear to have been produced by Tiversa to the Committee but not to the FTC. Please also send this to Laura VanDruff, who is cc'd on the letter as Complaint Counsel for the FTC.

Feel free to call Tyler or me if you have any questions.

Thanks,
Jen

Jennifer Barblan
Senior Counsel
Committee on Oversight and Government Reform
Rep. Darrell E. Issa, Chairman
(202) 225-5074
Jennifer.Barblan@mail.house.gov

Kelly, Andrea

From: Vandecar, Kim
Sent: Monday, December 01, 2014 1:08 PM
To: 'Barblan, Jennifer'; Bumpus, Jeanne
Cc: Grimm, Tyler
Subject: RE: Letter from Chairman Issa

Thank you Jen. We will make sure it gets to the Chairwoman and Ms. VanDruff.

From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Monday, December 01, 2014 1:05 PM
To: Bumpus, Jeanne; Vandecar, Kim
Cc: Grimm, Tyler
Subject: Letter from Chairman Issa

Jeanne and Kim –

I hope you both had a nice Thanksgiving. Attached please find a letter from Chairman Issa, accompanied by documents discussed within the letter that appear to have been produced by Tiversa to the Committee but not to the FTC. Please also send this to Laura VanDruff, who is cc'd on the letter as Complaint Counsel for the FTC.

Feel free to call Tyler or me if you have any questions.

Thanks,
Jen

Jennifer Barblan
Senior Counsel
Committee on Oversight and Government Reform
Rep. Darrell E. Issa, Chairman
(202) 225-5074
Jennifer.Barblan@mail.house.gov

RX637

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Wednesday, December 03, 2014 10:53 AM
To: Shonka, David C.; Vandecar, Kim
Subject: Draft reply to Chairman Issa
Attachments: Response123.docx

Dave and Kim,

Heather asked me to work with Don on a reply to Chairman Issa. Please let me know if you have any edits to the attached draft.

Jeanne

RX638

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Tuesday, December 02, 2014 3:42 PM
To: Clark, Donald S.
Cc: Vandecar, Kim
Subject: RE: Letter from Chairman Issa

Thanks Don.

From: Clark, Donald S.
Sent: Tuesday, December 02, 2014 3:28 PM
To: Bumpus, Jeanne
Cc: Vandecar, Kim
Subject: RE: Letter from Chairman Issa

Jeanne, thanks; (b)(5)

(b)(5)

Don

From: Bumpus, Jeanne
Sent: Tuesday, December 02, 2014 2:49 PM
To: Clark, Donald S.
Cc: Vandecar, Kim
Subject: FW: Letter from Chairman Issa

Don,

Attached is the letter from Chairman Issa we discussed this morning. It has already been shared with Laura Van Druff.

Jeanne

From: Barblan, Jennifer [<mailto:Jennifer.Barblan@mail.house.gov>]
Sent: Monday, December 01, 2014 1:05 PM
To: Bumpus, Jeanne; Vandecar, Kim
Cc: Grimm, Tyler
Subject: Letter from Chairman Issa

Jeanne and Kim –

I hope you both had a nice Thanksgiving. Attached please find a letter from Chairman Issa, accompanied by documents discussed within the letter that appear to have been produced by Tiversa to the Committee but not to the FTC. Please also send this to Laura VanDruff, who is cc'd on the letter as Complaint Counsel for the FTC.

Feel free to call Tyler or me if you have any questions.

Thanks,
Jen

Jennifer Barblan

RX638

Senior Counsel
Committee on Oversight and Government Reform
Rep. Darrell E. Issa, Chairman
(202) 225-5074
Jennifer.Barblan@mail.house.gov

RX639

Kelly, Andrea

From: Clark, Donald S.
Sent: Friday, December 19, 2014 4:50 PM
To: (b)(6)
Cc: Taylor, Susan; Helisek, Emalea R. CTR
Subject: Copy of Response To Chairman Issa
Attachments: SP60252_KMC14122002420.pdf

(b)(6) as we discussed, here's a copy of the response to Chairman Issa for your files. Both sides in the LabMD case and the Administrative Law Judge have now been given copies of the incoming letter, so there is no longer an ex parte contact issue; Sue and Emalea therefore will now scan the incoming letter and this response into DocSmart (but not circulate it to anyone else). Thanks for your call!

Don



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580


Office of the Secretary

December 16, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Issa:

Please know that because the matter of LabMD, Inc is still in administrative adjudication, your letter of December 1, 2014 has not been shared with the Chairwoman or the Commissioners. However, Chairwoman Ramirez has asked me to write and thank you on her behalf. Please also know, that after advising your Committee staff, the FTC's Complaint Counsel shared your letter with the Administrative Law Judge in the LabMD, Inc. matter, and with counsel for LabMD and Tiversa. Thank you again for sharing your findings.

Sincerely,

Donald S. Clark
Secretary of the Commission

RX640

Kelly, Andrea

From: Hipsley, Heather
Sent: Monday, December 15, 2014 5:19 PM
To: Ramirez, Edith
Subject: RE: Response129.docx

Great; thanks, H.

From: Ramirez, Edith
Sent: Monday, December 15, 2014 4:55 PM
To: Hipsley, Heather
Subject: Re: Response129.docx

Heather, I've made a couple of small changes. The revised text is below.


(b)(5)



From: Hipsley, Heather
Sent: Monday, December 15, 2014 04:10 PM
To: Ramirez, Edith
Subject: FW: Response129.docx

Hi Edith, I forgot that we haven't cleared this letter yet to go from Don back to Issa. Here's the text:

(b)(5)



(b)(5)



H.

From: Hipsley, Heather
Sent: Wednesday, December 10, 2014 5:38 PM
To: Ramirez, Edith
Subject: Response129.docx

I've edited the response letter to Issa a bit; Jeanne had forgotten to send it our way so just got this afternoon. H.

RX643

Kelly, Andrea

From: Clark, Donald S.
Sent: Monday, December 15, 2014 6:28 PM
To: Bumpus, Jeanne
Subject: RE: Slightly Revised Draft Response To Chairman Issa

Tracking:	Recipient	Delivery
	Bumpus, Jeanne	Delivered: 12/15/2014 6:28 PM

OK, will do; thanks!

... Don

From: Bumpus, Jeanne
Sent: Monday, December 15, 2014 6:27 PM
To: Clark, Donald S.
Subject: RE: Slightly Revised Draft Response To Chairman Issa

Don, (b)(5) Thanks.

From: Clark, Donald S.
Sent: Monday, December 15, 2014 6:20 PM
To: Bumpus, Jeanne
Subject: Slightly Revised Draft Response To Chairman Issa

Jeanne, I've attached a slightly revised version of the above response for your review, (b)(5)
(b)(5) Thanks!

... Don

CATEGORY 5

FTC communications

RX583


Kelly, Andrea

From: Sheer, Alain
Sent: Tuesday, October 28, 2014 1:36 PM
To: White, Christian S.
Subject: FW: FTC v. LabMD Docket No. 9357
Attachments: (b)(5)

Hi Chris. (b)(5)

From: VanDruff, Laura Riposo
Sent: Tuesday, October 28, 2014 10:47 AM
To: LabMD-Team; Schoshinski, Robert; Mithal, Maneesha
Subject: FW: FTC v. LabMD Docket No. 9357

(b)(5)



Kelly, Andrea

From: Clark, Donald S.
Sent: Tuesday, October 14, 2014 6:36 PM
To: White, Christian S.
Subject: FW: In Re LabMD Docket No. 9357
Attachments: (b)(5)

(b)(5)

Chris, (b)(5)
(b)(5)
(b)(5) Thanks!

Don

From: Mack, Julie
Sent: Thursday, October 09, 2014 3:27 PM
To: Shonka, David C.; White, Christian S.
Cc: Clark, Donald S.; Frankle, Janice Podoll
Subject: FW: In Re LabMD Docket No. 9357

Hello, Dave and Chris:

Please see below. (b)(5)
(b)(5) Please let me know. Thanks.

Julie

(b)(5)

Kelly, Andrea

From: Clark, Donald S.
Sent: Thursday, October 09, 2014 3:31 PM
To: Mack, Julie; Shonka, David C.; White, Christian S.
Cc: Frankle, Janice Podoll
Subject: Re: In Re LabMD Docket No. 9357

Chris, (b)(5) Thanks!

Don



Duplicate

Kelly, Andrea

From: Schoshinski, Robert
Sent: Friday, August 15, 2014 4:12 PM
To: White, Christian S.
Subject: VM: Schoshinski, Robert (3219)
Attachments: Voice_Message_Recording_S1234049_001_gsm.wav

Kelly, Andrea

From: Sheer, Alain
Sent: Thursday, August 14, 2014 2:48 PM
To: White, Christian S.
Subject: VM: Sheer, Alain (3321)
Attachments: Voice_Message_Recording_S1233067_001_gsm.wav

RX590

Kelly, Andrea

From: Mithal, Maneesha
Sent: Friday, June 27, 2014 10:51 AM
To: White, Christian S.
Subject: FW: (b)(5)
Attachments: (b)(5)

From: Blodgett, Katrina Ane
Sent: Thursday, June 26, 2014 2:35 PM
To: Mithal, Maneesha
Subject: (b)(5)

Maneesha-

Attached please find a memo (b)(5)
(b)(5)

Thank you,
Katrina

Katrina Blodgett
Division of Privacy and Identity Protection
Federal Trade Commission
202-326-3158

Kelly, Andrea

From: Mithal, Maneesha
Sent: Monday, June 23, 2014 10:34 AM
To: White, Christian S.
Subject: VM: Mithal, Maneesha (2771)
Attachments: Voice_Message_Recording_S1194273_001_gsm.wav

RX591

Kelly, Andrea

From: Mithal, Maneesha
Sent: Friday, June 20, 2014 8:54 AM
To: White, Christian S.
Cc: Sheer, Alain; VanDruff, Laura Riposo; Yodaiken, Ruth; Blodgett, Katrina Ane; Lincicum, David; Cohen, Kristin; Cox, Megan; Mehm, Ryan; Brown, Jarad; Lassack, Maggie
Subject: names of people at meeting yesterday

Hi Chris – I'm cc'ing the people who attended the meeting yesterday, per your request. Please keep us posted. Thanks!

Kelly, Andrea

From: Ramirez, Edith
Sent: Friday, June 20, 2014 8:18 AM
To: Nuechterlein, Jon; White, Christian S.
Subject: RE: LabMD

See you then. Thanks.

From: Nuechterlein, Jon
Sent: Friday, June 20, 2014 8:17 AM
To: White, Christian S.; Ramirez, Edith
Subject: Re: LabMD

I am.

From: White, Christian S.
Sent: Friday, June 20, 2014 07:17 AM
To: Ramirez, Edith; Nuechterlein, Jon
Subject: Re: LabMD

10:00 would work if Jon is available.

From: Ramirez, Edith
Sent: Friday, June 20, 2014 07:15 AM
To: White, Christian S.; Nuechterlein, Jon
Subject: RE: LabMD

Chris, I forgot about that... I can also meet at 10am or 3pm... Let me know what works... Thanks.

From: White, Christian S.
Sent: Friday, June 20, 2014 7:08 AM
To: Ramirez, Edith; Nuechterlein, Jon
Subject: Re: LabMD

I'm supposed to go with Jeanne, Kim V, Maneesha, Daniel K for a public briefing of Cong. Terry's staff at 11. Could we meet before that? Or, they could certainly get along w/o me.

From: Ramirez, Edith
Sent: Friday, June 20, 2014 06:54 AM
To: Nuechterlein, Jon; White, Christian S.
Subject: LabMD

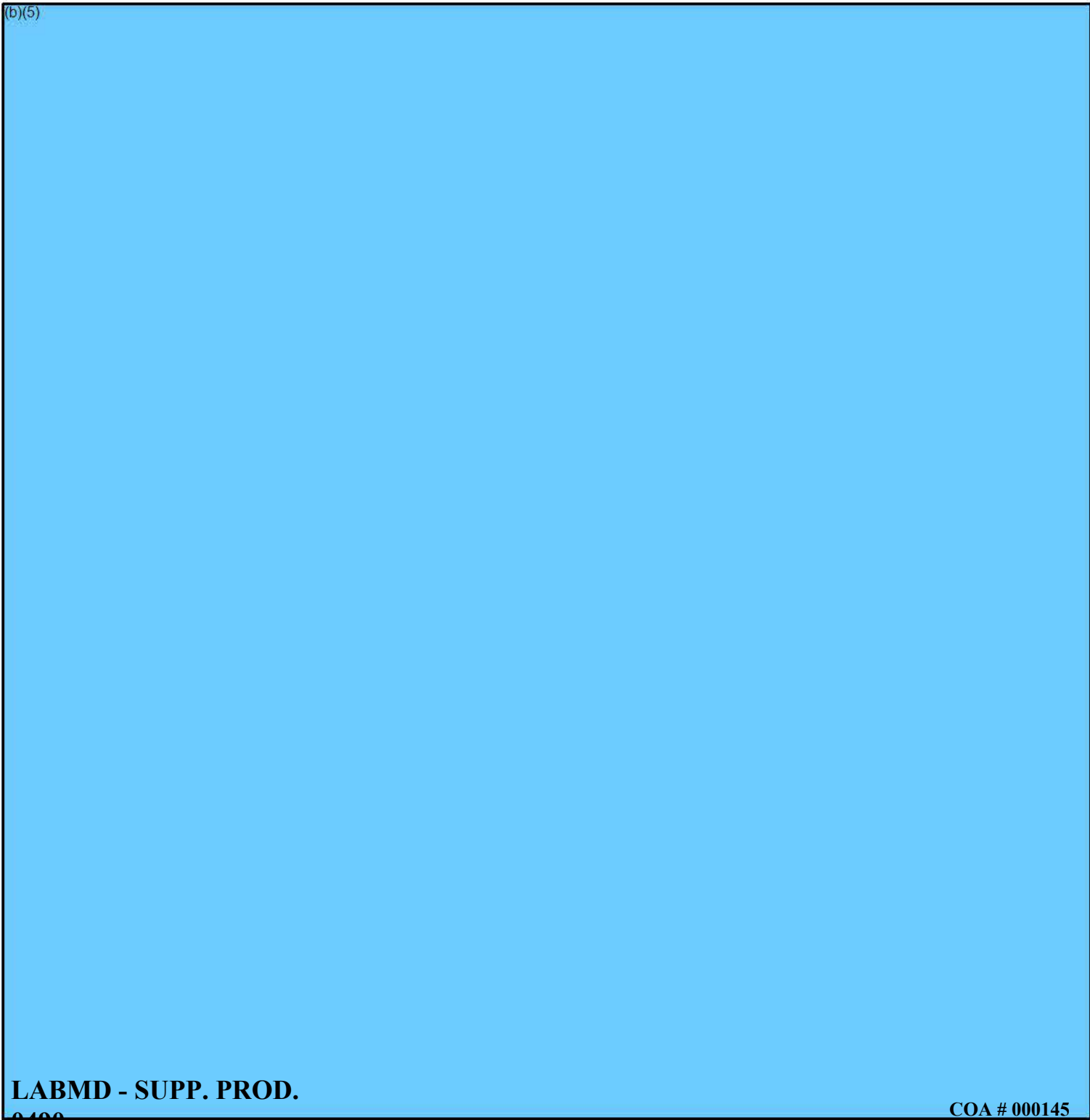
Jon & Chris, are you available to meet with me at 11am today about this Hill matter? Please let me know. Thanks.

RX595

Kelly, Andrea

From: Sheer, Alain
Sent: Wednesday, November 05, 2014 3:07 PM
To: White, Christian S.
Subject: filed yesterday.
Attachments: (b)(5)

(b)(5)



RX597

Kelly, Andrea

From: Sheer, Alain
Sent: Tuesday, June 10, 2014 2:18 PM
To: White, Christian S.
Subject: RE: (b)(5) [Redacted] Thanks. Alain

Thanks Chris

From: White, Christian S.
Sent: Tuesday, June 10, 2014 2:17 PM
To: Sheer, Alain
Subject: RE: (b)(5) [Redacted] Thanks. Alain.

From: Sheer, Alain
Sent: Tuesday, June 10, 2014 2:15 PM
To: White, Christian S.
Subject: (b)(5) [Redacted] Thanks. Alain.

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Tuesday, June 10, 2014 11:01 AM
To: White, Christian S.
Cc: Schoshinski, Robert
Subject: (b)(5)
Attachments: (b)(5)

As you discussed with Bob (b)(5)

Best,

Laura

Laura Riposo VanDruff
Federal Trade Commission
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W., NJ-8100
Washington, DC 20580
202.326.2999 (direct)
202.326.3062 (facsimile)
lvandruff@ftc.gov

RX598

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Wednesday, November 05, 2014 10:46 AM
To: White, Christian S.
Subject: (b)(5)

Attachments:



RX599

Kelly, Andrea

From: Schoshinski, Robert
Sent: Monday, June 09, 2014 3:15 PM
To: White, Christian S.
Subject: VM: Schoshinski, Robert (3219)
Attachments: Voice_Message_Recording_S1184624_001_gsm.wav

RX600

Kelly, Andrea

From: Sheer, Alain
Sent: Monday, June 02, 2014 9:21 AM
To: White, Christian S.
Subject: RE:

Hi Chris. (b)(5)
(b)(5) Alain...

From: White, Christian S.
Sent: Saturday, May 31, 2014 1:58 PM
To: Sheer, Alain
Subject: Fw:

Fyi...

From: Hipsley, Heather
Sent: Friday, May 30, 2014 10:37 PM
To: Bumpus, Jeanne; Cole, Justin; White, Christian S.
Subject: Fw:

Fyi. (b)(5) H

(b)(5),(b)(6)



RX602

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Tuesday, March 25, 2014 6:30 PM
To: White, Christian S.
Cc: Schoshinski, Robert
Subject: (b)(5)
Attachments: (b)(5)

Good evening, Chris.

(b)(5)

Best regards,

Laura

(b)(5)

RX603

Kelly, Andrea

From: Yodaiken, Ruth
Sent: Friday, March 14, 2014 2:18 PM
To: White, Christian S.
Subject: RE: (b)(5)

(b)(5)

Thanks,
Ruth

From: White, Christian S.
Sent: Friday, March 14, 2014 2:01 PM
To: Yodaiken, Ruth
Subject: (b)(5)

(b)(5)

RX604

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Tuesday, November 04, 2014 12:51 PM
To: White, Christian S.
Subject: call

Chris,

If you're up for a short conversation, will you please give me a call? I want to fill you in on a small development.

Best,

Laura

Laura Riposo VanDruff
Federal Trade Commission
Assistant Director, Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W., CC-8232
Washington, DC 20580
202.326.2999 (direct)
202.326.3393 (facsimile)
lvandruff@ftc.gov

RX606

Kelly, Andrea

From: Sieradzki, David L.
Sent: Monday, March 10, 2014 10:29 AM
To: Daly, John F.; Hegedus, Mark S.; Nuechterlein, Jon; Freedman, Bruce; Shonka, David C.
Cc: Cohen, William E.; White, Christian S.
Subject: (b)(5)
Attachments: (b)(5)

(b)(5)

David L. Sieradzki
Attorney, Office of General Counsel
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
office: 202.326-2092
fax: 202.326.2477

From: Daly, John F.
Sent: Tuesday, February 04, 2014 1:32 PM
To: Hegedus, Mark S.; Nuechterlein, Jon; Freedman, Bruce; Shonka, David C.
Cc: Sieradzki, David L.; Cohen, William E.; White, Christian S.
Subject: RE: LabMD motion for document subpoena on FTC Commissioners

(b)(5)

From: Hegedus, Mark S.
Sent: Tuesday, February 04, 2014 1:23 PM
To: Nuechterlein, Jon; Freedman, Bruce; Shonka, David C.
Cc: Sieradzki, David L.; Daly, John F.; Cohen, William E.
Subject: FW: LabMD motion for document subpoena on FTC Commissioners

Adding in Jon, Bruce and Dave.

(b)(5)

From: Sieradzki, David L.
Sent: Tuesday, February 04, 2014 1:14 PM
To: Shonka, David C.; Daly, John F.; Cohen, William E.; Hegedus, Mark S.
Subject: LabMD motion for document subpoena on FTC Commissioners

(b)(5)

Kelly, Andrea

From: Yodaiken, Ruth
Sent: Tuesday, March 04, 2014 4:22 PM
To: White, Christian S.
Subject: RE: (b)(5)

(b)(5)

Thanks,
Ruth

From: White, Christian S.
Sent: Thursday, February 27, 2014 4:32 PM
To: VanDruff, Laura Riposo; Yodaiken, Ruth
Subject: (b)(5)

(b)(5)

Kelly, Andrea

From: White, Christian S.
Sent: Monday, February 10, 2014 3:32 PM
To: Daly, John F.; Hegedus, Mark S.; Shonka, David C.
Subject: RE: (b)(5)

(b)(5)

From: Daly, John F.
Sent: Monday, February 10, 2014 3:23 PM
To: Hegedus, Mark S.; White, Christian S.; Shonka, David C.
Subject: Re: (b)(5)

(b)(5)

From: Hegedus, Mark S.
Sent: Monday, February 10, 2014 02:57 PM
To: Daly, John F.; White, Christian S.; Shonka, David C.
Subject: RE: (b)(5)

(b)(5)

Duplicate

Kelly, Andrea

From: Hegedus, Mark S.
Sent: Tuesday, February 04, 2014 1:56 PM
To: Sieradzki, David L.; Daly, John F.; Nuechterlein, Jon; Freedman, Bruce; Shonka, David C.
Cc: Cohen, William E.; White, Christian S.
Subject: RE: (b)(5)

(b)(5)

From: Sieradzki, David L.
Sent: Tuesday, February 04, 2014 1:49 PM
To: Daly, John F.; Hegedus, Mark S.; Nuechterlein, Jon; Freedman, Bruce; Shonka, David C.
Cc: Cohen, William E.; White, Christian S.
Subject: RE: (b)(5)

(b)(5)

Duplicate

Kelly, Andrea

From: White, Christian S.
Sent: Tuesday, February 04, 2014 1:20 PM
To: Daly, John F.
Subject: RE: (b)(5)

Thanks.

From: Daly, John F.
Sent: Tuesday, February 04, 2014 1:17 PM
To: White, Christian S.
Subject: FW: (b)(5)

I thought you should also see this, in light of our discussion this morning.

Duplicate



Kelly, Andrea

From: White, Christian S.
Sent: Tuesday, February 04, 2014 12:21 PM
To: Liu, Josephine
Subject: (b)(5)
Attachments: [Redacted]

From: VanDruff, Laura Riposo
Sent: Monday, February 03, 2014 11:18 AM
To: White, Christian S.
Cc: Schoshinski, Robert
Subject: (b)(5) [Redacted]

Good morning, Chris.

(b)(5) [Redacted]

Best regards,

Laura

Laura Riposo VanDruff
Federal Trade Commission
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W., NJ-8100
Washington, DC 20580
202.326.2999 (direct)
202.326.3062 (facsimile)
lvandruff@ftc.gov

Kelly, Andrea

From: White, Christian S.
Sent: Monday, February 03, 2014 4:15 PM
To: Freedman, Bruce
Subject: (b)(5)
Attachments: [Redacted]

From: VanDruff, Laura Riposo
Sent: Monday, February 03, 2014 11:18 AM
To: White, Christian S.
Cc: Schoshinski, Robert
Subject: (b)(5) [Redacted]

Good morning, Chris.

(b)(5) [Redacted]

Best regards,

Laura

Laura Riposo VanDruff
Federal Trade Commission
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W., NJ-8100
Washington, DC 20580
202.326.2999 (direct)
202.326.3062 (facsimile)
lvandruff@ftc.gov

RX610

Kelly, Andrea

From: Nuechterlein, Jon
Sent: Thursday, December 26, 2013 10:08 AM
To: Shonka, David C.; White, Christian S.; Daly, John F.; Freedman, Bruce; Cohen, William E.; Sieradzki, David L.; Grossman, Bradley D.
Subject: Fw: LabMD
Attachments: Brill Statement Re LabMD for filing.pdf

Fyi -- here is Commissioner Brill's disqualification statement, which has been emailed to the parties but not yet posted. Thanks to those who helped on this. - Jon

From: Tabor, April
Sent: Thursday, December 26, 2013 10:00 AM
To: Nuechterlein, Jon
Cc: Clark, Donald S.; Frankle, Janice Podoll
Subject: RE: LabMD

Hi Jon,

Commissioner Brill did end up filing a statement on Tuesday, which is attached. It was sent to the parties on Tuesday via email and FedEx. However, it has not yet been posted to the website because the Commissioner asked that we hold off posting until further notice. I expect we will receive further instructions later today.

Best,
April

-----Original Message-----

From: Nuechterlein, Jon
Sent: Thursday, December 26, 2013 9:55 AM
To: Tabor, April
Subject: LabMD

Hi April -- did Commissioner Brill end up filing a statement on Tuesday? If so, could you send it to me? Thanks!

Kelly, Andrea

From: Nuechterlein, Jon
Sent: Wednesday, December 18, 2013 5:50 PM
To: Kestenbaum, Janis; White, Christian S.
Subject: RE: LabMD

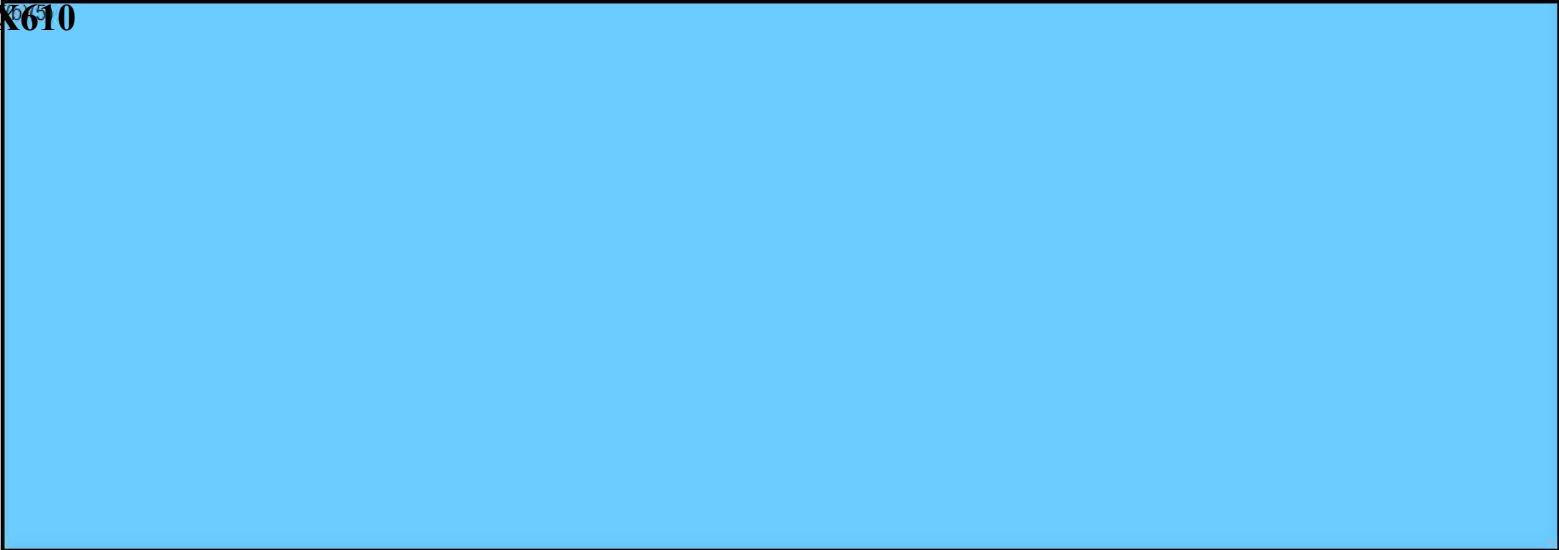
Chris will be on an airplane tomorrow morning en route to Tahoe. We just tried to call you; if you're around, please call. Otherwise, let's shoot for tomorrow afternoon, either between 2 and 3:30 or after 5.

From: Kestenbaum, Janis
Sent: Wednesday, December 18, 2013 5:36 PM
To: White, Christian S.; Nuechterlein, Jon
Subject: LabMD

Chris – I'd like to speak to you about this case. Do you have time tomorrow at 11? Jon, if you're free too, that would be great, but if not and Chris is available at 11, let's go ahead.

Thanks,
Janis

Janis Claire Kestenbaum | Federal Trade Commission
Office: (202) 326-2798 | Mobile: (202) 460-6261



From: Clark, Donald S.
Sent: Tuesday, December 17, 2013 5:20 PM
To: Tabor, April
Subject: FW: In the Matter of LabMD, Docket No. 9357: Respondent LabMD, Inc.'s Motion to Disqualify Commissioner Brill From This Administrative Proceeding

From: Michael Pepson [<mailto:michael.pepson@causeofaction.org>]
Sent: Tuesday, December 17, 2013 3:26 PM
To: Secretary; Clark, Donald S.
Subject: In the Matter of LabMD, Docket No. 9357: Respondent LabMD, Inc.'s Motion to Disqualify Commissioner Brill From This Administrative Proceeding

Dear Secretary Clark:

Please find attached to this e-mail a courtesy copy of Respondent LabMD, Inc.'s Motion to Disqualify Commissioner Brill from this Administrative Proceeding, which was filed today using the Federal Trade Commission E-Filing System.

Thank you.

Sincerely,

Michael Pepson

Michael D. Pepson | Counsel | Cause of Action
1919 Pennsylvania Avenue NW, Suite #650
Washington, D.C. 20006

Admitted to practice only in Maryland, the U.S. District Court for the District of Maryland, the U.S. District Court for the District of Colorado, the U.S. Court of Appeals for the D.C. Circuit, the U.S. Court of Appeals for the Ninth Circuit, and the U.S. Court of Appeals for the Eleventh Circuit. Practice limited to cases in federal court and administrative proceedings before federal agencies.

Michael.Pepson@causeofaction.org

O: [202.499.2024](tel:202.499.2024) |

Confidentiality: The information contained in this communication may be confidential, is intended only for the use of the recipient named above, and may be legally privileged. It is not intended as legal advice and may not be relied upon or used as legal advice. This communication does not establish an attorney-client relationship between us. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please re-send this communication to the sender and delete the original message and any copy of it from your computer system. Thank you.

RX655



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection
Division of Advertising Practices

Carl H. Settlemyer, III
202 326 2019 (Direct)
202 326 3259 (Fax)
csettlemyer@ftc.gov

June 25, 2008

VIA EMAIL AND REGULAR MAIL

Robert Boback, Chief Executive Officer
Tiversa, Inc.
144 Emeryville Drive, Suite 300
Cranberry Township, PA 16066

Dear Mr. Boback:

This notifies you of an official request for information that the Federal Trade Commission has received from Chairman Waxman of the Committee on Oversight and Government Reform of the House of Representatives. The Committee has requested information concerning inadvertent file sharing over peer-to-peer ("P2P") networks. Certain information and materials that Tiversa submitted may be responsive to this request.

The Commission routinely receives official requests for confidential information from congressional committees and subcommittees. Neither the Freedom of Information Act, 5 U.S.C. § 552(d), nor the Federal Trade Commission Act, 15 U.S.C. § 57b-2(d)(1)(A), authorize the Commission to withhold such information from congressional committees or subcommittees. The Commission, of course, requests that the responsive information and materials be kept confidential by the congressional committees and subcommittees.

If you have any questions about the Committee's inquiry or handling of information it has requested, please direct them to Committee staff contact, Roger Sherman, at (202) 225-5051. Questions about the Commission's response may be directed to me at (202) 326-2019.

Sincerely,

A handwritten signature in black ink, appearing to read "Carl H. Settlemyer".

Carl H. Settlemyer

cc: Office of General Counsel

RX659

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580



Bureau of Consumer Protection
Division of Advertising Practices

August 19, 2010

Mr. George Searle, CEO
Lime Wire LLC
45 Howard St.
New York, NY 10013

Re: Lime Wire LLC, FTC File No. 082-3046

Dear Mr. Searle:

The staff of the Federal Trade Commission has conducted an investigation of the LimeWire file-sharing application that put consumers' personal information in peril. As you know, users of some versions of LimeWire risk inadvertently sharing sensitive information stored on their computers. Consumers should not have to worry that one small mistake in configuring a software program such as LimeWire might expose their tax returns, credit reports, and college loan applications to millions of people. Identity thieves have used LimeWire to retrieve this information and injure consumers.¹ Ongoing research shows consumers continue to inadvertently share sensitive documents via peer-to-peer software, either through LimeWire or similar software applications.² It is imperative that distributors of such software act more responsibly and provide safeguards against inadvertent sharing.

During our investigation, we inquired whether Lime Wire LLC could force security upgrades for consumers who have installed legacy versions of LimeWire to help reduce these risks. Upon review of the matter, including non-public information submitted to the staff, we have determined not to recommend any further action by the Commission at this time. Among the factors we considered are Lime Wire's incorporation of safeguards against the inadvertent sharing of sensitive, personal documents into the user interface of more recent versions of its

¹ Press Release, United States Attorney's Office - W.D. Wash., Seattle Man Who Used Peer-to-Peer File Sharing Software to Steal Personal Info Sentenced to Prison (Aug. 11, 2009), available at <http://www.justice.gov/usao/waw/press/2009/aug/wood.html>.

² Press Release, Federal Trade Commission, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), available at <http://www.ftc.gov/opa/2010/02/p2palert.shtm>.

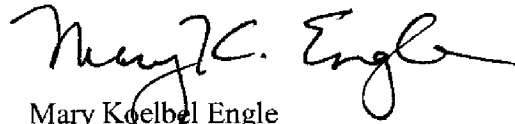
Mr. George Searle
August 19, 2010
Page 2

software; our understanding that the attrition rate for legacy versions is substantial; the apparent inability of Lime Wire to force users to upgrade legacy versions of the software to more recent versions; and the possibility that users of some of the older versions of LimeWire may have been able to avoid disclosure of sensitive information.³

We remain concerned, however, about consumers who are still using insecure legacy versions and are therefore subject to a risk of inadvertent sharing of sensitive, personal information. We expect Lime Wire to continue to advise consumers to upgrade legacy versions of its software because of the potential safety benefits of doing so, and to participate in software industry efforts to inform consumers about how best to avoid the inadvertent sharing of sensitive documents. Based on that expectation, it appears that no further action by the FTC staff is warranted at this time and the investigation is closed.

This action is not to be construed as a determination that a violation of law did not occur. The Commission reserves the right to take such further action as the public interest may require.

Very truly yours,



Mary Koelbel Engle
Associate Director

cc: Chul Pak, Esq.

³ See 15 U.S.C. § 45(n) (stating that an act or practice is not unfair unless, among other things, it causes “injury to consumers which is not reasonably avoidable by consumers themselves”).

EXHIBIT 1

CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY
Pursuant to 28 U.S.C. § 1746

1. I, Patrick Joseph Massari, have personal knowledge of the facts set forth below and am competent to testify as follows:
2. I have authority to certify the authenticity of the records produced by the Federal Trade Commission pursuant to proper Freedom of Information Act Requests issued on behalf of Cause of Action Institute under 5 U.S.C. § 552, from which select records are attached hereto as Appendix A.
3. The documents attached hereto as Appendix A are true and correct copies of documents as produced by the Federal Trade Commission to Cause of Action and maintained in the regular course of business.

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

Executed on 12 June, 2015.

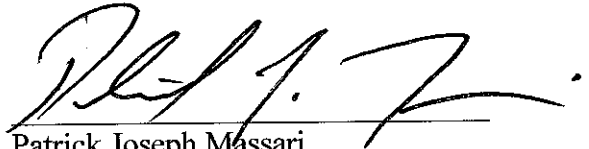

Patrick Joseph Massari
Counsel
Cause of Action Institute

EXHIBIT 2

December 24, 2013

Via e-mail and Regular mail
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

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

Dear Sir or Madam:

This letter is to notify you that counsel for LabMD, Inc. (“LabMD”), has issued a Request for Production of Documents and LabMD’s First Interrogatories to the Federal Trade Commission, which are enclosed. The Federal Trade Commission’s Rules of Practice state that “[a]ny party may serve on another party a request: to produce and permit the party making the request, or someone acting on the party’s behalf, to inspect and copy any designated documents or electronically stored information, as defined in §3.34(b), or to inspect and copy, test, or sample any tangible things which are within the scope of §3.31(c)(1) and in the possession, custody, or control of the party upon whom the request is served...” 16 C.F.R § 3.37(a). Accordingly, LabMD’s counsel has issued a Request for Production of Documents for certain of the FTC’s documents. The Rules of Practice further state that “[a]ny party may serve upon any other party written interrogatories ... to be answered by the party served or, if the party served is a public or private corporation, partnership, association or governmental agency, by any officer or agent, who shall furnish such information as is available to the party...” 16 C.F.R § 3.35(a). Accordingly, LabMD’s counsel has issued LabMD’s First Interrogatories.

On August 29, 2013, the Federal Trade Commission, Office of Administrative Law Judges issued a Protective Order Governing Discovery Material (the “Protective Order”) in the above-referenced action. The Protective Order protects confidential information produced in discovery in the case. A copy of the Protective Order signed by Chief Administrative Law Judge D. Michael Chappell is enclosed as an exhibit.

Any documents you produce to LabMD that are confidential must include the notice “CONFIDENTIAL – FTC Docket No. 9357,” in accordance with paragraph 6 of the Protective Order. If you produce confidential documents in electronic format, such as on a CD, thumb drive, or other media, you may place the “CONFIDENTIAL – FTC Docket No. 9357 designation on the CD, thumb drive, or other media.

I would be pleased to discuss any issues regarding responses or production of documents at your earliest convenience. You may reach me at (202) 372- 9100.

Sincerely,



William A. Sherman, II
Dinsmore & Shohl
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Phone: 202.372.9100
Fax: 202.372.9141
william.sherman@dinsmore.com
Counsel for Respondent LabMD

WAS:alm

Enclosures:

- (1) Request for Production of Documents
- (2) First set of Interrogatories
- (3) Exhibit A: Protective Order Governing Discovery Material
- (4) Exhibit B: Certification of Records of Regularly-Conducted Activity
- (5) Exhibit C: BCP Production Guide

cc (via email):

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm

Certificate of Service

I hereby certify that a duplicate original of the within Requests for Production and Interrogatories were duly served by e-mail and regular U.S. mail on the persons named herein on: December 24, 2013.

A handwritten signature in black ink that reads "William A. Sherman, II". The signature is written in a cursive style with a horizontal line underneath the text.

William A. Sherman, II
Dinsmore & Shohl
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Phone: 202.372.9100
Fax: 202.372.9141
william.sherman@dinsmore.com
Counsel for Respondent LabMD

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

**RESPONDENT LABMD, INC.'S FIRST SET OF
REQUESTS FOR PRODUCTION OF DOCUMENTS
COMPLAINT COUNSEL
(NUMBERS 1-17)**

Pursuant to the Federal Trade Commission’s Rules of Practice, 3.37, 16 C.F.R. § 3.37, and the Court’s Scheduling Order dated October 22, 2013, LabMD requests that Complaint Counsel produce the documents and material identified below for inspection and copying within thirty (30) days at the offices of Dinsmore & Shohl, LLP 801 Pennsylvania Avenue, N.W., Suite 610, Washington, D.C. 20004.

DEFINITIONS

1. **“All documents”** means each document within your possession, custody, or control, as defined below, that can be located, discovered or obtained by reasonable, diligent efforts, including without limitation all documents possessed by: (a) you, including documents stored in any personal electronic mail account, electronic device, or any other location under your control, or the control of your officers, employees, agents, or contractors; (b) your counsel; or (c) any other person or entity from which you can obtain such documents by request or which you have a legal right to bring within your possession by demand.

2. **“All communications”** means each communication, as defined below, that is a document that can be located, discovered, or obtained by reasonable, diligent efforts, including without limitation all communications possessed by: (a) you, including communications stored in any personal electronic mail account, electronic device, or any other location under your control, or the control of your officers, employees, agents, or contractors; (b) your counsel; or (c) any other person or entity from which you can obtain such

documents by request or that you have a legal right to bring within your possession by demand.

3. The term “**communication**” includes, but is not limited to, any transmittal, exchange, transfer, or dissemination of information, regardless of the means by which it is accomplished, and includes all communications, whether written or oral, and all discussions, meetings, telephone communications, or email contacts.
4. “**Complaint**” means the Complaint issued by the Federal Trade Commission in the above-captioned matter on August 28, 2013.
5. The term “**containing**” means containing, describing, or interpreting in whole or in part.
6. “**Dartmouth College**” means Dartmouth College, its divisions, programs, projects, affiliates, contractors, and its directors, officers, and employees.
7. “**Document**” means the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including, but not limited to, any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, journal, agenda, minute, code book or label. “**Document**” shall also include electronically stored information (“ESI”). **ESI** means the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created or stored information, including, but not limited to, electronic mail, instant messaging, videoconferencing, and other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, thumb or flash drives, cell phones, Blackberry, PDA, or other storage media, and such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.
8. The term “**documents sufficient to show**” means both documents that are necessary and documents that are sufficient to provide the specified information. If summaries, compilations, lists, or synopses are available that provide the information being requested, these may be provided in lieu of the underlying documents.

9. The terms “**each**,” “**any**,” and “**all**” shall be construed to have the broadest meaning whenever necessary to bring within the scope of any document request all documents that might otherwise be construed to be outside its scope
10. “**Federal Trade Commission**” or “**FTC**” means the Federal Trade Commission, and its directors, officers, and employees.
11. “**Includes**” or “**including**” means “including, but not limited to,” so as to avoid excluding any information that might otherwise be construed to be within the scope of any document request.
12. “**LabMD**” means LabMD, Inc., the named respondent in the above-captioned matter, and its directors, officers, and employees.
13. “**Or**” as well as “**and**” shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any document request all documents that otherwise might be construed to be outside the scope.
14. The term “**person**” means any natural person, corporate entity, partnership, association, joint venture, governmental entity, or other legal entity.
15. “**Personal information**” means individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a “cookie” or processor serial number.
16. Documents that are in your “**possession, custody, or control**” include, but are not limited to, documents that are in your constructive possession, custody, or control, as well as documents that are in the possession, custody, or control of your attorney (if not privileged or work product). This means that the documents do not need to be owned, written, or recorded by you to fall within this definition, which should be construed liberally.
17. The terms “**relate**” or “**relating to**” or “**referring or relating to**” mean discussing, constituting, commenting, containing, concerning, embodying, summarizing, reflecting, explaining, describing, analyzing, identifying, stating, referring to, dealing with, or in any way pertaining to, in whole or in part.

18. **“Sacramento Police Department”** means the Sacramento Police Department and its officials, employees, and agents.
19. **“Tiversa”** means Tiversa Holding Corporation, its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, Board members, officers, employees, agents, consultants, attorneys, and other persons working for or on behalf of the foregoing.
20. **“You”** or **“your”** means Federal Trade Commission.
21. **“1,718 File”** means the 1,718 page file Tiversa Holding Corporation (“Tiversa”) found on a peer-to-peer network and identified as having been created and stored on a LabMD computer
22. The use of the singular includes the plural, and the plural includes the singular.
23. The use of a verb in any tense shall be construed as the use of the verb in all other tenses.
24. Words in the masculine, feminine, or neuter form shall include each of the other genders.

INSTRUCTIONS

1. **Applicable Time Period:** Unless otherwise specified, the time period covered by a document request shall be limited to the period from January 1, 2005 to present.
2. **Objections:** Pursuant to Commission Rule of Practice § 3.37(b), any objection and reason therefore must be filed within thirty (30) days of service thereof.
3. **Protective Order:** On August 29, 2013, the Court entered a Protective Order governing discovery material in this matter. A copy of the protective order is enclosed as Exhibit A, with instructions on the handling of confidential information.
4. **Document Identification:** Documents that may be responsive to more than one specification of this Request for Production of Documents need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. Documents should be produced in the order in which they appear in your files or as electronically stored and without being manipulated or otherwise rearranged; if documents are removed from their original folders, binders, covers, containers, or electronic source in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, container, or electronic media or file paths from which such documents came. In

addition, number by page (or file, for those documents produced in native electronic format) all documents in your submission, preferably with a unique Bates identifier, and indicate the total number of documents in your submission.

5. **Production of Copies:** Unless otherwise stated, legible photocopies (or electronically rendered images or digital copies of native electronic files) may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this Request for Production of Documents. Further, copies of originals may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to LabMD or its counsel upon request. Copies of materials shall be produced in color if necessary to interpret them or render them intelligible.
6. **Sensitive Personally Identifiable Information:** If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please contact LabMD's counsel named above before sending those materials to discuss ways to protect such information during production. For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number *in combination with* one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
7. **Scope of Search:** These requests relate to documents that are in your possession or under your actual or constructive custody or control, including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, directors, officers, employees, or other agents or consultants, whether or not such documents were received from or disseminated to any other person or entity.
8. **Claims of Privilege:** Pursuant to the Federal Trade Commission's Rule of Practice 3.38(a), 16 C.F.R. § 3.38(a), if any documents are withheld from production based on a claim of privilege or any similar claim, you shall provide, not later than the date set for production of materials, a schedule that describes the nature of the documents,

communications, or tangible things not produced or disclosed in a manner that will enable LabMD's counsel to assess the claim of privilege. The schedule shall state individually for each item withheld: (a) the document control number(s); (b) the full title (if the withheld material is a document) and the full file name (if the withheld material is in electronic form); (c) a description of the material withheld (for example, a letter, memorandum, or email), including any attachments; (d) the date the material was created; (e) the date the material was sent to each recipient (if different from the date the material was created); (f) the email addresses, if any, or other electronic contact information to the extent used in the document, from which and to which each document was sent; (g) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all authors; (h) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all recipients of the material; (i) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all persons copied on the material; (j) the factual basis supporting the claim that the material is protected (for example, that it was prepared by an attorney rendering legal advice to a client in a confidential communication, or prepared by an attorney in anticipation of litigation regarding a specifically identified claim); and (k) any other pertinent information necessary to support the assertion of protected status by operation of law. If only part of a responsive document is privileged, all non-privileged portions of the document must be produced.

9. **Certification of Records of Regularly Conducted Activity:** Attached as Exhibit B is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena you to testify at future proceedings in order to establish the admissibility of documents produced in response to this Request for Production of Documents. You are asked to execute this Certification and provide it with your response.
10. **Continuing Nature of Requests:** This request for documents shall be deemed continuing in nature so as to require production of all documents responsive to any specification included in this request produced or obtained by you prior to the close of discovery, which is currently scheduled for March 5, 2014.
11. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this Request for Production of Documents. We may require the submission of additional documents at a later time. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this litigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise.

Electronic Submission of Documents: The following guidelines refer to the production of any Electronically Stored Information (“ESI”) or digitally imaged hard copy documents. Before submitting any electronic production, you must confirm with LabMD counsel named above that the proposed formats and media types will be acceptable to LabMD. LabMD requests Concordance load-ready electronic productions, including DAT and OPT load files.

12. **Electronically Stored Information:** Documents created, utilized, or maintained in electronic format in the ordinary course of business should be delivered to LabMD as follows:

- (a) Spreadsheet and presentation programs, including but not limited to Microsoft Access, SQL, and other databases, as well as Microsoft Excel and PowerPoint files, must be produced in native format with extracted text and metadata. Data compilations in Excel spreadsheets, or in delimited text formats, must contain all underlying data un-redacted with all underlying formulas and algorithms intact. All database productions (including structured data document systems) must include a database schema that defines the tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, Java, XML schemas, and other elements, including the use of any report writers and custom user data interfaces;

All ESI other than those documents described in (l)(a) above must be provided in native electronic format with extracted text or Optical Character Recognition (“OCR”) and all related metadata, and with corresponding image renderings as converted to Group IV, 300 DPI, single-page Tagged Image File Format (“TIFF”) or as color JPEG images (where color is necessary to interpret the contents); and

- (b) Each electronic file should be assigned a unique document identifier (“DocID”) or Bates reference.

(1) **Hard Copy Documents:** Documents stored in hard copy in the ordinary course of business should be submitted in an electronic format when at all possible. These documents should be true, correct, and complete copies of the original documents as converted to TIFF (or color JPEG) images with corresponding document-level OCR text. Such a production is subject to the following requirements:

- (a) Each page shall be endorsed with a document identification number (which can be a Bates number or a document control number); and
 - (b) Logical document determination should be clearly rendered in the accompanying load file and should correspond to that of the original document; and
 - (c) Documents shall be produced in color where necessary to interpret them or render them intelligible.
- (2) For each document electronically submitted to LabMD, you should include the following metadata fields in a standard ASCII delimited Concordance DAT file:
- (a) For electronic mail: begin Bates or unique document identification number (“DocID”), end Bates or DocID, mail folder path (location of email in personal folders, subfolders, deleted or sent items), custodian, from, to, cc, bcc, subject, date and time sent, date and time received, and complete attachment identification, including the Bates or DocID of the attachments (“AttachIDs”) delimited by a semicolon, MD5 or SHA Hash value, and link to native file;
 - (b) For email attachments: begin Bates or DocID, end Bates or DocID, parent email ID (Bates or DocID), page count, custodian, source location/file path, file name, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file;
 - (c) For loose electronic documents (as retrieved directly from network file stores, hard drives, etc.): begin Bates or DocID, end Bates or DocID, page count, custodian, source media, file path, filename, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file; and
 - (d) For imaged hard-copy documents: begin Bates or DocID, end Bates or DocID, page count, source, and custodian; and where applicable, file folder name, binder name, attachment range, or other such references, as necessary to understand the context of the document as maintained in the ordinary course of business.

(3) If you intend to utilize any de-duplication or email threading software or services when collecting or reviewing information that is stored in your computer systems or electronic storage media, or if your computer systems contain or utilize such software, you must contact LabMD's counsel named above to determine whether and in what manner you may use such software or services when producing materials in response to this Request for Production of Documents.

(4) Submit electronic productions as follows:

- (a) With passwords or other document-level encryption removed or otherwise provided to LabMD;
- (b) As uncompressed electronic volumes on size-appropriate, Windows-compatible media;
- (c) All electronic media shall be scanned for and free of viruses;
- (d) Data encryption tools may be employed to protect privileged or other personal or private information. LabMD accepts TrueCrypt, PGP, and SecureZip encrypted media. The passwords should be provided in advance of delivery, under separate cover. Alternate means of encryption should be discussed and approved by LabMD; and
- (e) Please mark the exterior of all packages containing electronic media sent through the U.S. Postal Service or other delivery services as follows:

**MAGNETIC MEDIA- DO NOT X-RAY
MAY BE OPENED FOR POSTAL INSPECTION.**

(5) All electronic files and images shall be accompanied by a production transmittal letter, which includes:

- (a) A summary of the number of records and all underlying images, emails, and associated attachments, native files, and databases in the production; and
- (b) An index that identifies the corresponding consecutive document identification number(s) used to identify each person's documents and, if submitted in paper form, the box number containing such documents. If the index exists as a computer file(s), provide the index both as a printed hard copy and in machine-readable form (provided that LabMD's counsel

named above determines prior to submission that the machine-readable form would be in a format that allows LabMD to use the computer files). We have included a Bureau of Consumer Protection Production Guide as Exhibit C. This guide provides detailed directions on how to fully comply with this instruction.

13. **Documents No Longer In Existence:** If documents responsive to a particular specification no longer exist for reasons other than the ordinary course of business or the implementation of your document retention policy but you have reason to believe have been in existence, state the circumstances under which they were lost or destroyed, describe the documents to the fullest extent possible, state the specification(s) to which they are responsive, and identify Persons having knowledge of the content of such documents.
14. **Incomplete Records:** If you are unable to answer any question fully, supply such information as is available. Explain why such answer is incomplete, the efforts made by you to obtain the information, and the source from which the complete answer may be obtained. If books and records that provide accurate answers are not available, enter best estimates and describe how the estimates were derived, including the sources or bases of such estimates. Estimated data should be followed by the notation "est." If there is no reasonable way for you to make an estimate, provide an explanation.
15. **Questions:** Any questions you have relating to the scope or meaning of anything in this request or suggestions for possible modifications thereto should be directed to William A. Sherman, II at 202.372.9100.
16. Documents responsive to the request shall be addressed to the attention of William A. Sherman, II, Dinsmore & Shohl LLP, 801 Pennsylvania Ave., NW, Suite 610, Washington, DC 20004, and delivered between 8:30 a.m. and 5:00 p.m. on any business day.

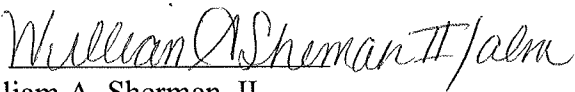
REQUESTS

Please produce the following:

1. All documents referring or relating to the 1,718 File.
2. All communications between Dartmouth College and FTC.
3. All communications between M. Eric Johnson and FTC.
4. All communications between Tiversa and FTC.
5. All communications between FTC and any third person not employed by FTC referring or relating to LabMD or the 1,718 File.
6. All communications between FTC and any federal Government agency, including the U.S. Department of Homeland Security, concerning LabMD generally and/or the 1,718 File specifically.
7. All communications between FTC employees referring or relating to LabMD or the 1,718 File that is not protected as attorney work product, including communications between the FTC and the FTC's Office of Public Affairs (including communications between the FTC and the Office of Public Affairs's current and former employees).
8. All documents sufficient to show what data-security standards are currently used by FTC to enforce the law under Section 5 of the Federal Trade Commission Act.
9. All documents sufficient to show what changes occurred in the data-security standards used by FTC to enforce the law under Section 5 of the Federal Trade Commission Act from 2005 to the present and the dates on which these standards changed.
10. All documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present.
11. All documents provided to the FTC pursuant to any Civil Investigation Demand regarding its investigation of LabMD.
12. All documents identifying LabMD and other companies whose documents or files Tiversa downloaded from Peer to Peer Networks which contained Personal Identifying Information and or Protected Health Information that were provided to FTC.
13. All documents identifying consumers that were harmed, or that are substantially likely to be harmed, as result of the claims alleged against LabMD in the Complaint.

14. All documents that are utilized by FTC to determine whether to pursue an investigation or complaint against an entity or individual, including but not limited to evaluation standards and scoring systems.
15. All communications and all documents relating to communications between FTC and the Sacramento Police Department from October 5, 2012 to the present.
16. All communications—including letters—between FTC and the Persons identified in the documents discovered by the Sacramento Police Department at 5661 Wilkinson Street, Sacramento, CA, on October 5, 2012; Bates-Labeled by the FTC in the present matter as FTC-SAC-000233 through 000272, FTC-SAC-000273 through 000282, and FTC-SAC-000001 through 000044.
17. All documents relating to communications between the Bureau of Competition and the Persons identified in documents discovered by the Sacramento Police Department at 5661 Wilkinson Street, Sacramento, CA, on October 5, 2012; Bates-Labeled by the FTC in the present matter as FTC-SAC-000233 through 000272, FTC-SAC-000273 through 000282, and FTC-SAC-000001 through 000044.

December 24, 2013

By: 
William A. Sherman, II
Dinsmore & Shohl
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Phone: 202.372.9100
Fax: 202.372.9141
william.sherman@dinsmore.com
Counsel for Respondent LabMD

CERTIFICATE OF SERVICE

This is to certify that on December 24 2013, I served via email a copy of the foregoing document to:

Alain Sheer
Attorney
Federal Trade Commission
600 Pennsylvania Ave, NW
Room NJ-8100
Washington, DC 20580
Phone: 202-326-3321
Fax Number: 202-326-3062
Email: asheer@ftc.gov

Laura Riposo VanDruff
Attorney
Federal Trade Commission
600 Pennsylvania Ave, NW
Room NJ-8100
Washington, DC 20580
Phone: 202-326-2999
Fax Number: 202-326-3062

Megan Cox
Attorney
Federal Trade Commission
600 Pennsylvania Ave, NW
Room NJ-8100
Washington, DC 20580
Phone: 202-326-2282
Fax Number: 202-326-3062

Margaret Lassack
Attorney
Federal Trade Commission
600 Pennsylvania Ave, NW
Room NJ-8100
Washington, DC 20580
Phone: 202-326-3713
Fax Number: 202-326-3062

Ryan Mehm
Attorney
Federal Trade Commission
600 Pennsylvania Ave, NW
Room NJ-8100
Washington, DC 20580
Phone: 202-326-3713
Fax Number: 202-326-3062

December 24, 2013

By: 
William A. Sherman, II

EXHIBIT 3

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

LabMD, INC.,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No.: _____
)	
FEDERAL TRADE COMMISSION,)	
)	
Defendant.)	
_____)	

DECLARATION OF MICHAEL D. PEPSON

The undersigned declarant, Michael D. Pepson, states:

1. I am an attorney at Cause of Action Institute, counsel for the plaintiff LabMD, Inc. (“LabMD”). The following facts are based on my own personal knowledge and, if called as a witness, I could and would testify competently thereto.

2. Attached hereto as Exhibit 1 is a true and correct copy of a publicly available document on PHIprivacy.net entitled “Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated),” which is available at <http://www.phiprivacy.net/meanwhile-back-in-court-tiversa-sues-labmd-for-defamation-seeks-to-block-publication-of-book-by-labmd-ceo/> (last visited March 17, 2014).

3. Attached hereto as Exhibit 2 is a true and correct copy of a publicly available press release posted on the Federal Trade Commission's (the "FTC") website, entitled "FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy" (Aug. 29, 2013), which is available at <http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers> (last visited March 17, 2014).

4. Attached hereto as Exhibit 3 is a true and correct copy of the following publicly available document, which is posted on the FTC's Business Center Blog: Lesley Fair, entitled "FTC files data security complaint against LabMD (Aug. 29, 2013), at <http://www.business.ftc.gov/blog/2013/08/ftc-files-data-security-complaint-against-labmd> (last visited Mar. 17, 2014).

5. Attached hereto as Exhibit 4 is a true and correct copy of a publicly available excerpt of a speech given by Federal Trade Commissioner Julie Brill on September 17, 2013, entitled "Forum Europe Fourth Annual EU Data Protection and Privacy Conference, Commissioner Julie Brill's Keynote Address," which is available on the FTC's website at http://www.ftc.gov/sites/default/files/documents/public_statements/keynote-address-forum-europe-fourth-annual-eu-data-protection-and-privacy-conference/130917eudataprivacy.pdf (last visited Mar. 17, 2014).

6. Attached hereto as Exhibit 5 is a true and correct copy of an excerpt of a publicly available speech given by Federal Trade Commissioner Julie Brill on October 29, 2013, entitled “Commissioner Julie Brill's Opening Panel Remarks, European Institute, Data Protection, Privacy and Security: Re-Establishing Trust Between Europe and the United States,” which is available on the FTC’s website at http://www.ftc.gov/sites/default/files/documents/public_statements/data-protection-privacy-security-re-establishing-trust-between-europe-united-states/131029europeaninstituteremarks.pdf (last visited Mar. 17, 2014).

7. Attached hereto as Exhibit 6 is a true and correct copy of an excerpt of a publicly available speech given to the International Association of Privacy Professionals by the FTC’s Director of the Bureau of Competition, Jessica Rich, on December 6, 2013, entitled “Privacy Today and the FTC’s 2014 Privacy Agenda,” which is available on the FTC’s website at http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-today-ftcs-2014-privacy-agency/131206privacytodayjrich.pdf (last visited Mar. 17, 2014).

8. Attached hereto as Exhibit 7 is a true and correct copy of an excerpt of a publicly available speech given by Federal Trade Commissioner Maureen K. Ohlhausen on September 14, 2013, entitled “The FTC’s Privacy Agenda for the

2014 Horizon, Forum for EU-US Legal-Economic Affairs,” which is available on the FTC’s website at http://www.ftc.gov/sites/default/files/documents/public_statements/ftc%20%80%99s-privacy-agenda-2014-horizon-forum-eu-u.s.legal-economic-affairs/130914berlinprivacyin2014.pdf (last visited Mar. 17, 2014).

9. Attached hereto as Exhibit 8 is a true and correct copy of an excerpt of the deposition transcript of Ms. Letonya Randolph, who was deposed on February 4, 2014, as a Federal Rule of Civil Procedure 30(b)(6)-type witness for Midtown Urology, Inc., in the In the Matter of LabMD, Inc., FTC Dkt. No. 9357, with particularly relevant portions highlighted.

10. Attached hereto as Exhibit 9 is a true and correct copy of an excerpt of a publicly available AP News article authored by Anne Flaherty entitled “FTC: Medical Lab’s Lax Security Led to Data Leak” (August 29, 2013), which is available on the Bloomberg Businessweek website at <http://www.businessweek.com/ap/2013-08-29/ftc-medical-labs-lax-security-led-to-data-breach> (last visited Mar. 17, 2014).

11. Attached hereto as Exhibit 10 is a true and correct copy of an excerpt of a publicly available AdWeek article authored by Katy Bachman, entitled “FTC’s Jessica Rich Lays Out Ambitious Ad Enforcement Agenda” (Sept. 30, 2013), which is

available at <http://www.adweek.com/news/advertising-branding/ftcs-jessica-rich-lays-out-ambitious-ad-enforcement-agenda-152794> (last visited Mar. 17, 2014).

12. Attached hereto as Exhibit 11 is a true and correct copy of excerpts from Complaint Counsel's Response to LabMD, Inc.'s First Set of Interrogatories (Numbers 1-22), In the Matter of LabMD, Inc., Dkt. No. 9357 (Jan. 24, 2014).

13. Attached hereto as Exhibit 12 is a true and correct copy of excerpts from Complaint Counsel's Answer and Objections to Respondent's First Set of Requests for Production of Documents (Numbers 1-17), In the Matter of LabMD, Inc., Dkt. No. 9357 (Jan. 24, 2014).

14. Attached hereto as Exhibit 13 is a true and correct copy of excerpts from Complaint Counsel's Response to LabMD, Inc.'s First Set of Requests for Admission (Numbers 1-20), In the Matter of LabMD, Inc., Dkt. No. 9357 (Mar. 3, 2014).

15. Attached hereto as Exhibit 14 is a true and correct copy of a letter sent by FTC enforcement staff to LabMD's counsel on March 3, 2014, Re: In the Matter of LabMD, Inc. Docket No. 9357.

16. Attached hereto as Exhibit 15 is a true and correct copy of document produced to LabMD's counsel on March 3, 2014, as responsive to LabMD's

Request for Production 10 (FTC-103115), entitled “NIST.OCR HIPAA Security Rule June 6 2012 (with notes).pptx.”

17. Attached hereto as Exhibit 16 is a true and correct copy of an excerpt from the following June 6, 2012, FTC Power Point presentation: Cora Tung Han, FTC, Division of Privacy and Identity Protection, NIST/OCR HIPAA Security Rule Conference (June 6, 2012). This document is publicly available at http://abouthipaa.com/wp-content/uploads/day1-2_chan_ftc-privacy-report.pdf (last visited Mar. 19, 2014), and is available through a hyperlink on the related website, <http://abouthipaa.com/about-hipaa/hipaa-hitech-resources/nist-ocr-2012-hipaa-security-conference-presentations/> (last visited Mar. 19, 2014) entitled “Beyond HIPAA: The FTC Privacy Report.”

18. Attached hereto as Exhibit 17 is a true and correct copy of an excerpt from the following document: Complaint Counsel’s Motion for Protective Order Regarding Rule 3.33 Notice of Deposition, In the Matter of LabMD, FTC Dkt. No. 9357 (Feb. 14, 2014).

19. Attached hereto as Exhibit 18 is a true and correct copy of the Expert Report of Raquel Hill, Ph.D., which was provided to LabMD’s counsel on March 18, 2014, in In the Matter of LabMD, Inc., FTC Dkt. No. 9357.

20. Attached hereto as Exhibit 19 is a true and correct copy of a document entitled “Division of Privacy and Identity Protection,” which is publicly available on the Federal Trade Commission’s website at <http://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity> (last visited Mar. 19, 2014).

21. I have highlighted particularly relevant portions of Exhibits 4, 5, 6, 7, 8, 10, and 17 to this declaration.

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

Executed on March 20, 2014

/s/ Michael D. Pepson
Michael D. Pepson

EXHIBIT 1

- Home
- About/Contact
- Privacy Policy & TOS

Featured Articles

- NHS sells a billion patient records
- Louisiana lawmakers want to keep a state database of people who have medication-induced abortions
- Audit finds high-risk security vulnerabilities in the automated systems used to process Medicaid claims
- WA: Skagit County Government Settles Potential HIPAA Violations

Recent Posts

- Service Coordination Inc. also affected MD Department of Health and Mental Hygiene patients
- Business associate of Maryland Developmental Disabilities Administration hacked in October
- Where there's a breach, there's a lawsuit
- AZ: Hospitalists of Arizona laptop stolen from St. Mary's Hospital contained patient information
- NHS sells a billion patient records
- Leader of Stolen Identity Refund Fraud Ring Sentenced to Jail
- CO: Valley View Hospital hacked; 5400 patients affected
- Meanwhile, in the LabMD case...
- UK: Home care agency warned after vulnerable people's details left in the street
- StayWell breach affects over 12,000; how many more not disclosed (update1)

Recent Comments

- Trish Harkness on Leader of Stolen Identity Refund Fraud Ring Sentenced to Jail
- Dissent on StayWell breach affects over 12,000; how many more not disclosed (update1)
- dewluca on StayWell breach affects over 12,000; how many more not disclosed (update1)

News Sections

Archives

Sep 09 2013

Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated)

Article or Commentary, Breaches

Back in July, I reported that **LabMD had unsuccessfully attempted to sue Tiversa in Georgia** for allegedly stealing its property. At issue was a file containing PHI on 1,178 patients that Tiversa had downloaded as part of a research project after the file was exposed via P2P software on LabMD's system. In its 2009 **press release** on its research, Tiversa did not name LabMD, but the matter **eventually came to the FTC's attention**, who opened an investigation and took LabMD to court when it failed to fully comply with an investigative demand. LabMD was ordered to comply, and in August, the **FTC sued LabMD** for failure to adequately protect consumer information. LabMD **responded forcefully** to the complaint in a press statement, alluding to Tiversa as "Internet trolls." In other statements, they've described Tiversa in other unflattering terms.

Now it seems that Tiversa is suing LabMD. Erin McAuley reports:

A cyber-intelligence company and its CEO sued the author of the book "The Devil Inside the Beltway," claiming it falsely accused them of assisting "abusive government shakedowns" through "government-funded data mining & surveillance."

Tiversa Holding Corp. and its co-founder and CEO Robert Boback sued LabMD Inc. and its CEO/author Michael J. Daugherty, in Federal Court.

Daugherty's book is slated for publication on Sept. 17, by (nonparty) Broadland Press. Advance material published on the Internet identifies Daugherty as the CEO of LabMD.

[...]

Boback and Tiversa claim the book defames them: "In his video 'trailer' for the book, available on Mr. Daugherty's personal website, Mr. Daugherty highlights his position as LabMD's president and CEO and Mr. Daugherty alleges that Tiversa is part of a 'Government Funded Data Mining & Surveillance' scheme that engages in 'Psychological Warfare' and helps to assist in 'Abusive Government Shakedown[s].' See www.michaeljdaugherty.com. More specifically, Mr. Daugherty alleges Tiversa is conducting '300 Million Searches per day' for 'Homeland Security' and the 'Federal Trade Commission.'

Read more on [Courthouse News](#).

Seemingly lost in most of the legal wrangling is the fact that it seems that no one whose data were in the "1718 file" were notified of the P2P exposure under HIPAA because LabMD took the position that no breach (as defined by HIPAA in 2008) had occurred.

So is HHS investigating this at all? HHS has not yet responded to an email sent by PHlprivacy.net inquiring as to whether HHS had ever opened (or concluded) an investigation of this incident. This post will be updated when I receive a reply.

Update: An HHS spokesperson responded to my inquiry with the following statement:

OCR decided not to join FTC in their investigation of these p2p sharings and we did not independently receive complaints. As you note, this was pre-HITECH, so there was and is

no obligation on LabMD with respect to our breach notification requirements — whether any exist under state law would be for the state to determine.

Posted by Dissent at 3:32 pm

Tagged with: LabMD

4 Responses to “Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated)”

1. **David Szabo** says:

September 10, 2013 at 2:22 pm

The Interim Final Breach Breach Notification Rule did not become effective until September 2009. So if the breach occurred in 2008, is its unlikely that a report was required.

Dissent says:

September 10, 2013 at 2:40 pm

I suspect you're right, and I had made the same point in my [July post](#) about the incident pre-dating HITECH. But those data may now have been in a number of hands since HITECH went into effect, so what then? I would think that the PHI lost any HIPAA protection it might have had once it came into the FTC's hands, but how many parties have had access to the data since September 2009, and should HHS be looking into this?

Dissent says:

September 12, 2013 at 3:36 pm

HHS responded to my inquiry. See the update at the bottom of the post. You were correct.

2. **Doc Sheldon** says:

September 14, 2013 at 5:37 pm

I would think that Tiversa's counsel would have advised Mr. Boback that there's little hope of winning a case claiming slander, libel or defamation, when the subject statements can be proven to be true.

It also seems a bit difficult to base a lawsuit upon statements in a book that hasn't yet been published. I guess I'm just a stickler for details.

Sorry, the comment form is closed at this time.

ICS Collection Service, Inc. press release on data breach affecting University of Chicago Physicians Group patients

Update to the inVentiv/Adheris lawsuit against HHS over prescription refill reminder programs

Notice of Electronic Service

I hereby certify that on June 12, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s Motion to Admit Select Exhibits, with:

D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Ave., NW
Suite 110
Washington, DC, 20580

Donald Clark
600 Pennsylvania Ave., NW
Suite 172
Washington, DC, 20580

I hereby certify that on June 12, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s Motion to Admit Select Exhibits, upon:

John Krebs
Attorney
Federal Trade Commission
jkrebs@ftc.gov
Complaint

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Jarad Brown
Attorney
Federal Trade Commission
jbrown4@ftc.gov
Complaint

Kent Huntington
Counsel
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Sunni Harris
Esq.
Dinsmore & Shohl LLP
sunni.harris@dinsmore.com
Respondent

Daniel Epstein
Cause of Action
daniel.epstein@causeofaction.org
Respondent

Patrick Massari
Counsel
Cause of Action
patrick.massari@causeofaction.org
Respondent

Prashant Khetan
Senior Counsel
Cause of Action
prashant.khetan@causeofaction.org
Respondent

Alain Sheer
Federal Trade Commission
asheer@ftc.gov
Complaint

Laura Riposo VanDruff
Federal Trade Commission
lvandruff@ftc.gov
Complaint

Megan Cox
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov
Complaint

Erica Marshall
Counsel
Cause of Action
erica.marshall@causeofaction.org
Respondent

Patrick Massari
Attorney