

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION



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

ORIGINAL

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

DOCKET NO. 9357

PUBLIC

MOTION TO DISQUALIFY COMMISSIONER EDITH RAMIREZ

Pursuant to 16 C.F.R. § 4.17, Respondent LabMD, Inc. (“LabMD”) respectfully moves to disqualify Commissioner Edith Ramirez because she has been irrevocably tainted and compromised by her involvement in the Federal Trade Commission’s (“FTC” or “Commission”) response to the United States House of Representatives Committee on Oversight and Government Reform (“OGR”) investigation of Tiversa, Inc. (“Tiversa”).

Facts

A. **Background.**

On June 21, 2012, Commissioner J. Thomas Rosch prophetically warned FTC about Tiversa, stating “I do not agree that staff should further inquire – either by document request, interrogatory, or investigational hearing – about the 1,718 File.” Dissenting Statement of Commissioner J. Thomas Rosch, Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 (June 21, 2012), *available at* <https://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./1023099-labmd-full-commission-review-jtr-dissent.pdf>. He went on to note FTC’s obvious conflict of interest in

blindly relying upon “a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks.” *Id.*

FTC should have listened.

On September 25, 2013, the Administrative Law Judge (“ALJ”) advised LabMD’s counsel that all pre-hearing dispositive motions “will be ruled on by the Commission, the same body that voted to issue the complaint in this case.” Initial Pretrial Conference, at 7:12-14.

On November 21, 2013 and again on June 7, 2014, through the testimony of FTC’s lead witness, Tiversa CEO Robert Boback, LabMD discovered FTC had conspired with Tiversa to transfer stolen files, and that CX19, a one-page piece of paper with four typed IP addresses created for Boback’s testimony by Richard Wallace (the whistleblower granted immunity to testify in this case), was the *only* document “proving” that the 1718 File had been “found” on P2P networks and not been stolen from a LabMD computer. FTC had done nothing at all to corroborate Tiversa’s claims before launching its fishing expedition.¹

On November 8, 2013, Commissioner Wright published an article demonstrating how LabMD was statistically *certain* to lose its case, even if the ALJ, after hearing the evidence, ruled in its favor.²

¹ FTC had “twenty-first century law enforcement tools” including “Consumer Sentinel, a secure, online fraud and identity theft complaint database” and “Internet Lab, which provides FTC lawyers and investigators with high-tech tools to...capture web sites that come and go quickly...[providing] FTC staff with the necessary equipment to preserve evidence for presentation in court.” *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov’t Reform, 110th Cong. (July 24, 2007)* (statement of Mary Engle, Assoc. Dir. for Advertising Practices, Federal Trade Comm’n), at 3, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-peer-peer-file-sharing-technology-issues/p034517p2pshare.pdf. However, FTC did not verify the 1718 File’s origin.

² As Commissioner Wright recently reiterated: “Perhaps the most obvious evidence of abuse of process is the fact that over the past two decades, the Commission has almost exclusively ruled in favor of FTC staff....when the administrative law judge dares to disagree with FTC staff, the Commission almost universally reverses and finds liability.” Remarks of Joshua D. Wright, Global Antitrust Inst. Invitational Moot Court Competition, at 17 (Feb. 21, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/626231/150221judgingantitrust-1.pdf. Commissioner Wright further said that defending FTC is “facially implausible.” *Id.* at 18.

On December 24, 2013, Commissioner Brill “voluntarily” recused herself amid credible claims of bias against LabMD. *See* Respondent’s Motion To Disqualify Commissioner Brill, at 1-7, FTC Dkt. No. 9357 (Dec. 17, 2013); Statement of Commissioner Julie Brill, FTC Dkt. No. 9357 (Dec. 24, 2013).

On May 7, 2014, a federal judge described FTC’s case against LabMD as “unreasonable” and “almost being unconscionable.” *See* Hearing Tr., *LabMD v. FTC*, Case No. 1:14-cv-00810-WSD (N.D. Ga. May 9, 2014), at 91:20-21; 77:9-15; 80:3-22:

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

MR. SCHOSHINSKI: “That’s correct, Your Honor.”

...

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

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

THE COURT: “Are you serious about that last response?”

B. OGR Investigates FTC.

FTC’s ill-advised partnership with Tiversa caused Congress, for the first time in decades, to intervene in a pending administrative case. This investigation, in turn, caused Commissioners and staff to protect the agency. Responding to proper FOIA requests, FTC has withheld disclosure of a vast number of Commissioners’ emails, documents and other records, claiming the deliberative process privilege, which strongly suggests that the Commissioners were engaged in substantive discussions regarding the LabMD matter. It also has withheld other records given to Congress under the Speech or Debate Clause, suggesting FTC believes that an Article II Branch agency has Article I congressional power. However, the limited records FTC has produced demonstrate Commissioner Ramirez and her staff were fully engaged, contrary to her quasi-judicial responsibility.

On June 11, 2014, OGR notified FTC that both Tiversa and the Commission were under investigation and that the information Complaint Counsel used to prosecute LabMD was “incomplete and inaccurate.”³

Ramirez and FTC’s top leadership responded by drafting a one paragraph letter dated June 13, 2014, ostensibly from FTC’s Secretary Donald Clark. *See* Ex. 1, at 000091. Ramirez’s Chief of Staff Heather Hipsley and Senior Legal Advisor Janis Kestenbaum edited and finalized Clark’s letter: *“Don, here is the final with Edith’s input . . . Please provide a copy back to our office after you sign and send . . . Thanks! H.”*⁴

FTC’s internal communications show Ramirez’s involvement in the Congressional response effort.⁵ The initial e-mail from OGR Staff to Ramirez was received at 5:28 p.m., and forwarded to Jeanne Bumpus (Director, FTC Office of Congressional Relations) and Kim Vandecar (FTC congressional liaison) at 5:39 p.m.⁶ Bumpus then e-mailed Designated Agency Ethics Official (“DAEO”) Christian White at 6:13 p.m.,⁷ who sent Ramirez the letter at 6:30 p.m., and also forwarded it to General Counsel Jon Nuechterlein and Bruce Freedman (Assistant General Counsel for Ethics).⁸ Nuechterlein sent Hipsley the letter at 12:05 p.m. the next day with an “fyi.”⁹ Ramirez had the final say.¹⁰

On June 17, 2014, OGR asked FTC Acting Inspector General Kelly Tshibaka (the “AIG”) to investigate the FTC/Tiversa relationship:

³ *See* Ex. 1, documents produced by FTC in response to FOIA-2015-00109 (Feb. 19, 2015) (COA Bates #s 00001–00250), at 000092.

⁴ *Id.*, at 000144 (emphasis added); 000142–49.

⁵ *See* Ex. 2, documents produced by FTC in response to FOIA-2014-01217 Productions 1 (Aug. 25, 2014) and 2 (Sept. 11, 2014) (COA Bates #s 00001–00089), at 00048.

⁶ *See* Ex. 1, at 000151.

⁷ *Id.*, at 000150–51.

⁸ *Id.*, at 000150.

⁹ *Id.*

¹⁰ *Id.*, at 000146–49; 000139.

The possibility that inaccurate information played a role in the FTC's decision to initiate enforcement actions against LabMD is a serious matter....[T]he alleged collaboration between the FTC and Tiversa...creates the appearance that the FTC aided a company whose business practices allegedly involve disseminating false data about the nature of data security breaches.¹¹

The fire was raging and again Ramirez directed strategy.

On June 18, 2014, the AIG informed Ramirez about the June 17 letter.¹² Hipsley responded: "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."¹³

Hipsley, however, neglected to advise the AIG that Ramirez had dictated Clark's response.

Ramirez refused to be walled off. DAEO White briefed Hill staffer Shannon Taylor regarding FTC/Tiversa on June 20, and it appears Ramirez met White beforehand to discuss the briefing and the AIG's investigation.¹⁴ Ramirez certainly knew the AIG was investigating allegations of staff misconduct.¹⁵

On Friday, July 18, 2014, OGR sent Ramirez another letter, this time echoing Commissioner Rosch's warnings about Tiversa:¹⁶

Given what the Committee has learned so far, I have serious reservations about the FTC's reliance on Tiversa as a source of information....Because Tiversa was benefiting commercially from the fact that the FTC was investigating the companies that Tiversa itself referred[,]...it is critical for the Committee to understand the relationship between the FTC and Tiversa, and whether Tiversa manipulated the FTC[.]¹⁷

¹¹ *Id.*, at 000119.

¹² *See* Ex. 1, at 000127.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*, at 000124.

¹⁶ *Id.*, at 000082-88.

¹⁷ *Id.*, at 000082-84.

On July 21, 2014, the Commission was required to vote on the release of non-public material, including regarding LabMD, to OGR, which surprised staff.¹⁸ “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.” To vote, the Commission had to be familiar with the subject matter and substance.¹⁹

On July 23, 2014, Senator Jay Rockefeller sent OGR a letter berating its Chairman for interfering in the LabMD case.²⁰ It appears FTC instigated and may have even drafted this letter for Rockefeller’s staff,²¹ after weeks of cascading calls, meetings, and communications.²²

The Rockefeller letter was sent the day prior to OGR’s July 24 hearing,²³ where FTC was warned it would be “attacked.”²⁴ Ellen Doneski, a key Rockefeller aide, sent her friend “Edith” (Ramirez) a copy of the attack letter early in the afternoon of July 23, before it was made public.²⁵

A July 23 e-mail from Patrick Satalin (staffer for Rep. Peter Welch) to Aaron Burstein (Brill’s Attorney Advisor) shows how FTC gamed its congressional allies to deflect criticism:

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.²⁶

¹⁸ *Id.*, at 000100.

¹⁹ See FTC, Operating Manual, Ch. 15: *Confidentiality and Access*, available at https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch15confidentialityandaccess_0.pdf (last visited Apr. 27, 2015).

²⁰ See Ex. 2, at 00002-00003.

²¹ *Id.*, at 00009–00016.

²² *Id.*, at 00012–00018 (see, e.g., Taylor June 18, 2014 e-mail to Vandecar: “We definitely need to talk now.”).

²³ U.S. House of Rep., Comm. on Oversight & Gov’t Reform, *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury*, Full Committee (Jul. 24, 2014), available at <http://oversight.house.gov/hearing/federal-trade-commission-section-5-authority-prosecutor-judge-jury-2/> (last visited Apr. 27, 2015).

²⁴ See Ex. 2, at 00055.

²⁵ *Id.*, at 00001.

²⁶ *Id.* Commissioner Brill, of course, already had recused herself from the LabMD matter.

FTC's Hill operatives in both chambers chimed in:²⁷ “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?”²⁸

On December 1, 2014, OGR sent a fourth letter to Ramirez, proving that Tiversa withheld crucial documents from both FTC and OGR, that Boback perjured himself, and that Tiversa had obstructed the LabMD case by withholding responsive evidence.²⁹

Argument

I. The Decisionmaking Process Is Fatally Tainted.

Agency action is invalidated when the judgment of the ultimate decision-maker is improperly shaped by outside considerations. *See Aera Energy v. Salazar*, 642 F.3d 212, 221 (D.C. Cir. 2011); *Peter Kiewit Sons’ Co. v. United States Army Corps of Eng’rs*, 714 F.2d 163, 170 (D.C. Cir. 1983). Two principles guide the analysis. First, “the *appearance* of bias” is no less objectionable than the reality. *ATX v. Dep’t of Transp.*, 41 F.3d 1522, 1527 (D.C. Cir. 1994); *Pillsbury Co. v. Federal Trade Comm’n*, 354 F.2d 952, 963-65 (5th Cir.1966). For example, in *Koniag v. Andrus*, 580 F.2d 601, 610-11 (D.C. Cir. 1978), the Court found that one letter from Representative Dingell “compromised the appearance of the Secretary’s impartiality.” Second, if “extraneous pressure intruded into the calculus of consideration,” then a Commissioner must be disqualified. It is the nexus between the pressure and the decision-maker not the nature of the pressure that is decisive. *District of Columbia Fed’n of Civic Ass’ns v. Volpe*, 459 F.2d 1231, 1246 (D.C. Cir.), *cert. denied*, 405 U.S. 1030 (1972).³⁰

²⁷ *Id.*, at 00008–00011.

²⁸ *Id.*, at 00039.

²⁹ See Ex. 3, Letter from OGR Chairman Darrell Issa to FTC Chairwoman Edith Ramirez (Dec. 1, 2015), at 7.

³⁰ FTC has refused the remedy for such taint – full disclosure on the record. *See Aera Energy*, 646 F.3d at 220-21.

Generally, the cases involve claims of Congressional interference that caused agencies to act improperly. *See ATX*, 41 F.3d at 1522; *Pillsbury*, 354 F.2d at 963; *Koniag*, 580 F.2d at 601. Here, Congress pressured FTC to *stop* acting improperly, but the legal principle applies regardless.

OGR's letters questioned FTC's competence and professionalism. Now, only a judgment against LabMD will rescue FTC's reputation, for any other result confirms FTC's prosecutorial misconduct or malpractice and exposes the agency to civil liability. Furthermore, the few records FTC has produced show a definite nexus between the Congressional investigation and FTC's response with respect to this case. Therefore, FTC's decision-making process is "irrevocably tainted." *Lichoulas v. FERC*, 606 F.3d 769, 778 (D.C. Cir. 2010).

II. Ramirez Should Be Disqualified Because There Is A Reasonable Suspicion She Has Prejudged This Case.

The test for disqualification is whether a disinterested observer may conclude that the agency has in some measure pre-judged the facts and/or law. *Cinderella Career & Finishing Schools, Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970); *see also Nuclear Info. & Res. Set. v. NRC*, 509 F.3d 562, 571 (D.C. Cir. 2007); *Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1164-65 (D.C. Cir. 1995); <http://www.governmentattic.org/12docs/8FTC-OIGinvs2013.pdf> (IG report noting improper Commissioner communications). By claiming the deliberative process privilege as grounds to withhold Commissioners' records, FTC certainly creates the presumption that the facts of this case have been reviewed and adjudicated in some manner or fashion. And, no neutral judge would do what Ramirez (or FTC) did here: "It is fundamental that both unfairness and the appearance of unfairness should be avoided. **Wherever there may be reasonable suspicion of unfairness, it is best to disqualify.**" *Am. Cyanamid Co. v. FTC*, 363 F.2d 757, 767 (6th Cir. 1966) (emphasis added); *Marshall v. Jerrico, Inc.*, 446 U.S.

238, 242 (1980) (no person should be “deprived of his interests in the absence of a proceeding in which he may present his case with assurance that the arbiter is not predisposed to find against him”).

Conclusion

LabMD respectfully moves that Chairwoman Ramirez disqualify herself immediately and abstain from any further participation in this matter.

Dated: April 27, 2015

Respectfully submitted,



Daniel Z. Epstein
Prashant K. Khetan
Patrick J. Massari
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Telephone: 202.499.4232
Fax: 202.330.5842
Email: prashant.khetan@causeofaction.org



Reed D. Rubinstein
William A. Sherman, II
Dinsmore & Shoal, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Counsel for Respondent, LabMD, Inc.

EXHIBIT 1

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)

Chris, (b)(5)
(b)(5)
(b)(5) Thanks!

Don

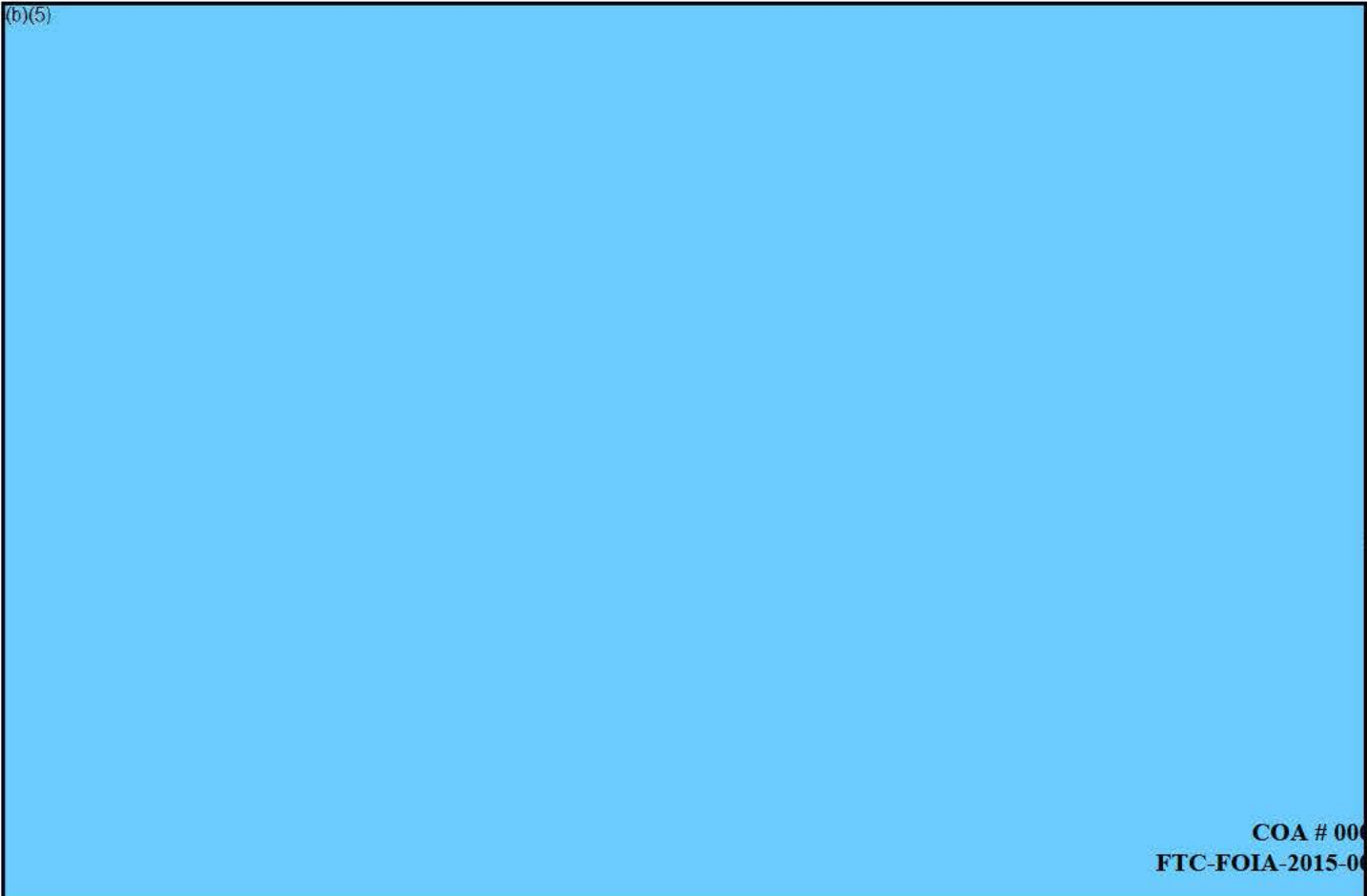
From: Mack, Julie
Sent: Thursday, October 09, 2014 3:27 PM
To: Shonka, David C.; White, Christian S.
Cc: Clark, Donald S.; Frankle, Janice Podoll
Subject: FW: In Re LabMD Docket No. 9357

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

3. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 2201, and 5 U.S.C. § 702. In LabMD v. FTC, Case No. 13-15267-F, at 2 (11th Cir. Feb. 18, 2014), the United States Court of Appeals for the Eleventh Circuit examined whether it had jurisdiction to entertain LabMD’s claims against the FTC under the APA, as codified in relevant part at 5 U.S.C. §§ 701-06, under the federal Constitution, and under 28 U.S.C. § 1331, which allows for “nonstatutory” review of ultra vires agency actions. The Court held:

[J]urisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted [by LabMD] at this stage, first must be asserted and considered in a district court.

(internal citations omitted). A true and correct copy of the foregoing Order is attached hereto as Exhibit 1 and is incorporated herein by reference. See also Sackett v. E.P.A., 132 S. Ct. 1367, 1373 (2012) (“... the APA provides for judicial review of all *final* agency actions”); id. at 1374 (“The Court holds that the Sacketts may immediately litigate their jurisdictional challenge in federal court. I agree, for the Agency has ruled definitively on that question.”) (Ginsburg, J. concurring). The grounds for the relief requested include the due process clause of the United States Constitution, 5 U.S.C. §§ 701-706 (APA’s judicial review provisions), 28 U.S.C. §

1651 (the All Writs Act), 28 U.S.C. § 2201 (the Declaratory Judgment Act), and 28 U.S.C. § 2202 (further relief).

4. The FTC has finally determined that it has jurisdiction over LabMD and that it has complied with constitutional due process fair-notice requirements: In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Jan. 16, 2014). A true and correct copy of the foregoing order is attached hereto as Exhibit 2 and is incorporated herein by reference.

5. The FTC claims the foregoing decision marks the consummation of its decisionmaking process, has the force of law, and is entitled to deference under “Chevron.” See Supplemental Letter Brief, FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD, Dkt. 152-1, at 6 (Jan. 21, 2014). A true and correct copy of the foregoing brief is attached hereto as Exhibit 3 and is incorporated herein by reference.

6. Venue is proper under 28 U.S.C. §1391(e).

NATURE OF THE CASE

7. LabMD, at all relevant times a small medical laboratory providing doctors with cancer-detection services, is now on the verge of ceasing all operations after being trapped in a paralyzing web of government investigations, subpoenas, and administrative litigation.

8. At some unknown point between 2005 and August 2013, the FTC, through enforcement activities and/or internet postings on the FTC's website, rather than through administrative rulemaking, guidance or known standards, declared for the first time that certain unspecified patient-information data-security practices employed by LabMD were inadequate and thus an "unfair" trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5").

9. The FTC still has yet to issue any rule or statement with legal force and effect describing the specific patient-information data-security practices it believes Section 5 prohibits or permits.

10. Between 2005 and the present, the FTC never specified in a rule or statement with legal force and effect how LabMD's patient-information practices fell short or described what, exactly, it should have done differently at any given point. In fact, the FTC commenced an investigation of LabMD in January 2010, filed its administrative complaint in August 2013, and still today, LabMD has yet to be told what, exactly, it did wrong at any point during the relevant period of years.

11. The FTC's actions and a campaign of disparagement, including conclusory statements by an FTC Commissioner that LabMD had mishandled sensitive patient information made shortly after the administrative complaint had been filed, have eviscerated LabMD's business and destroyed its professional reputation.

12. In October, 2013, LabMD lost its directors and officers (D&O) liability insurance as a result of the pending enforcement action and has been unable to obtain D&O insurance because of the pending action.

13. Further, LabMD and its doctors were denied “tail” medical malpractice insurance because of the FTC’s actions, which will, unless this matter is resolved favorably in the near future, severely limit LabMD’s prospects for obtaining medical malpractice insurance going forward and thus hiring qualified physicians.

14. The company’s insurance carrier has advised that it will not renew LabMD’s general liability insurance policy effective May 6, 2014, so that the policy will terminate effective October, 2014. This means that LabMD cannot rent office space.

15. The FTC’s actions have forced LabMD, a company that once employed more than forty people and provided diagnostic services to more than one hundred doctors, to stop accepting samples.

16. At all times relevant, LabMD’s Protected Health Information (“PHI”), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services (“HHS”) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act

(“HITECH”), 42 U.S.C. §§ 300jj et seq., 17901 et seq. See <http://www.healthit.gov/providers-professionals/ehr-privacy-security/practice-integration> .

17. Neither the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH. See Complaint, In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Aug. 28, 2013). A true and correct copy of the foregoing complaint is attached hereto as Exhibit 4.

18. Even if Section 5 does empower the FTC to broadly regulate data-security, which it does not, Congress delegated sole authority to regulate PHI data-security to the HHS. And even if Section 5 does empower the FTC to regulate PHI data-security concurrently with HHS and/or to “overfile” HHS using a “common law” of consent orders and internet posts to impose requirements in excess of those set through HHS rulemaking, which it does not, the Commission’s refusal to promulgate rules or regulations and provide the public with proper notice and comment violates LabMD’s due process rights by failing to give fair notice of what the FTC believes Section 5 forbids or requires.

19. Not only does the FTC lack the statutory authority to regulate PHI and/or cyber-security, it also lacks the expertise to do so. For example, Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” 78 Fed. Reg. 11739 (Feb.

19, 2013), available at <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf> (accessed Mar. 18, 2014), directed the Department of Commerce to set data-security standards, not the FTC.

20. To stop the abuse, LabMD seeks a declaration that the FTC lacks jurisdiction under Section 5 over PHI data-security practices and that the FTC has violated LabMD's due process and First Amendment rights. It also seeks preliminary and permanent injunctive relief staying the administrative proceedings in In the Matter of LabMD, Inc., FTC Dkt. No. 9357. Finally, LabMD asks that the FTC pay all of LabMD's attorneys' fees and litigation costs.

FACTS

21. Section 5 authorizes the FTC to prohibit "unfair or deceptive acts or practices in or affecting commerce."

22. The FTC in this case claims Section 5 "unfairness" authority to regulate LabMD's PHI data-security practices, even absent a claim of "deception," by way of administrative "common law" established through consent orders and Internet postings.

I. The FTC Targets LabMD.

23. In or about 2008, Tiversa Holding Corp. ("Tiversa"), a self-described "cyber-intelligence company" specializing in searching for and copying medical,

financial, and other sensitive files on peer-to-peer networks using patented technology, obtained a LabMD accounts-receivable computer file containing PHI without LabMD's knowledge or consent.

24. On May 13, 2008, Tiversa contacted LabMD, advised it that Tiversa had taken its property, and refused to provide information on the procurement of the file unless LabMD entered into a contract for Internet security services. LabMD turned down this offer. See Dissenting Statement of Commissioner J. Thomas Rosch, Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 (June 21, 2012). A true and correct copy of the foregoing dissent is attached hereto as Exhibit 5 and is incorporated herein by reference.

25. In 2009, Tiversa gave LabMD's PHI accounts-receivable file to the FTC under highly irregular circumstances. See id. Recent deposition testimony of Tiversa's CEO, Robert Boback, suggests the FTC and Tiversa met on multiple occasions and ultimately conspired and agreed to transfer LabMD's file via a FTC civil investigative demand (CID) to a third company (the "Privacy Institute") that, upon information and belief, is a company that has a relationship with a Tiversa advisory board member.

26. Beginning in January 2010, the FTC requested and LabMD voluntarily provided thousands of pages of documents and submitted to multiple meetings and interviews.

27. Then, on December 21, 2011, the FTC issued formal civil investigative demands (the “CIDs”) to LabMD.

28. LabMD filed a Petition to Limit or Quash the CIDs on January 10, 2012, explaining, among other things, that LabMD’s PHI data security was exclusively regulated by HHS and solely subject to HHS rules and regulations establishing data-security standards for PHI under HIPAA and HITECH.

29. Commissioner Julie Brill denied LabMD’s petition on April 20, 2012. Commission Letter Denying LabMD, Inc.’s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty’s Petition to Limit or Quash the Civil Investigative Demand, in File No. 1023099, at 13 (April 20, 2012). A true and correct copy of the foregoing correspondence is attached hereto as Exhibit 6 and is incorporated herein by reference.

30. Commissioner Brill acknowledged that LabMD’s PHI accounts-receivable spreadsheet file “can be considered” protected health information regulated under HIPAA and HITECH but claimed that the FTC jurisdiction under Section 5 was “overlapping and concurrent.” Id.

31. On April 25, 2012, LabMD appealed Commissioner Brill's ruling, arguing, as the Commission recently admitted, that the FTC "does not enforce HIPAA or HITECH." See Ex. 2 at 12 & n.19. LabMD also challenged the FTC's reliance on the PHI accounts-receivable file obtained from Tiversa.

32. Nonetheless, on June 21, 2012, three Commissioners (including Commissioner Brill) affirmed Commission Brill's ruling, "finding its conclusions to be valid and correct." See Commission Letter Affirming the Ruling, By Commissioner Brill, Denying the Petitions To Limit or Quash Filed by LabMD and Michael J. Daugherty (June 21, 2012). A true and correct copy of the foregoing order is attached hereto as Exhibit 7 and is incorporated herein by reference. Then-Commissioner Thomas Rosch dissented. Ex. 5.

33. The FTC then filed a petition to enforce the CIDs in this Court. LabMD opposed the petition, arguing, among other things, that the FTC lacked jurisdiction to regulate data-security.

34. The Hon. William S. Duffey upheld the CIDs, but said "there is significant merit" to LabMD's argument that Section 5 does not justify an investigation into data-security practices and consumer privacy issues. See Opinion and Order, FTC v. LabMD et al., 1:12-cv-3005-WSD, Dkt. No. 23, at 4 (N.D. Ga.

Nov. 26, 2012) (Duffy, J.). A true and correct copy of the foregoing order is attached hereto as Exhibit 8.

II. LabMD Publicly Criticizes The FTC And The FTC Retaliates.

35. LabMD's owner, Michael Daugherty decided to warn the public about the FTC's abuses through the press, social media, and a book. Mr. Daugherty used, and continues to use, his website, <http://michaeljdaugherty.com/>, to criticize the government.

36. For example, Mr. Daugherty was quoted in a September 7, 2012, Atlanta Business Chronicle article as follows: "We are guilty until proven innocent with these people They are on a fishing expedition. We feel like they are beating up on small business." Amy Wenk, "Atlanta Medical Lab Facing Off Against FTC," Atlanta Business Chronicle (September 5, 2012). Ms. Wenk wrote that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about \$500,000 fighting the investigation." Id.

37. On information and belief, FTC attorney Alain Sheer, who would later serve as lead counsel for the FTC in an enforcement action against Plaintiff, monitored Mr. Daugherty's political speech and retaliated against him for it.

38. For example, on July 19, 2013, Mr. Daugherty posted the trailer to his book, "The Devil Inside the Beltway," on his website,

<http://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/>.

The trailer called the FTC's actions against LabMD an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming . . . [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." It criticized Commission staff, including Mr. Sheer.

39. On July 22, 2013, Mr. Sheer told LabMD that Commission staff had recommended that the FTC commence enforcement proceedings against LabMD.

40. On July 30, 2013, Janis Claire Kestenbaum, the Senior Legal Advisor to the Chairwoman of the FTC, provided LabMD a draft complaint.

41. On August 28, 2013, the Commission commenced an enforcement action (the "Enforcement Action") by issuing a complaint and notice order. The gravamen of its claim at that time was about the PHI accounts-receivable file purloined by Tiversa. Mr. Sheer, who met with Tiversa and who was responsible for the shell-game through which the FTC obtained the file, is lead Complaint Counsel.

42. The FTC's Complaint in the Enforcement Action makes clear that LabMD was a "health care provider" and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things.

43. The FTC did not allege that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes.

44. Instead, the FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices. It said LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. See Ex. 4 ¶¶ 10-11.

45. The FTC did not name an individual complainant or allege direct harm to any person.

46. The FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively low cost."

47. The FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," allegedly violated Section 5.

48. The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security.

49. Mr. Sheer of the FTC has admitted that “[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward.” Initial Pretrial Conference Transcript, In the Matter of LabMD, Inc., Dkt. No. 9357, 10:11-15 (Sept. 25, 2013) (“Initial Pretrial Conf. Trans.”). He also acknowledged that the FTC brought this action without any complaining witnesses who say their data was released or disclosed. Id. 33:3-5. A true and correct copy of that transcript is attached hereto as Exhibit 9.

50. No court has ever held the FTC may require firms to adopt information-practice policies under Section 5's “unfairness” prong. Hearing Trans. 16: 22-25, FTC v. LabMD, Inc. et al., Case No. 1:12-cv-3005-WSD (Sept. 19, 2012) (Duffy, J.) (emphasis added). A true and correct copy is attached hereto as Exhibit 10.

51. On September 17, 2013, LabMD filed an answer challenging the FTC's jurisdiction and violations of LabMD's federal constitutional due process rights, among other things.

52. In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.

53. On October 24, 2013, Mr. Sheer of the FTC served a subpoena duces tecum on Mr. Daugherty, LabMD's CEO and President, requesting the following documents concerning Mr. Daugherty's book:

- "All drafts of . . . [Mr. Daugherty's book about the FTC] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" Mr. Daugherty's book about the FTC.
- "All documents related to the source material for drafts of" Mr. Daugherty's book about the FTC, "including documents referenced or quoted in the" book.
- "All promotional materials related to" Mr. Daugherty's book criticizing the FTC, "including, but not limited to, documents posted on social media, commercials featuring . . . [Mr. Daugherty], and presentations or interviews given by" Mr. Daugherty.

54. After over four years of investigation and litigation, LabMD still does not know when or what it did "wrong" and cannot even determine what the elements of a data-security "unfairness" offense are in this case.

55. For example, FTC enforcement staff have refused to substantively respond to LabMD's interrogatories regarding PHI data-security standards—including "data-security standards, regulations, and guidelines the FTC seeks to enforce against LabMD"—except to cross-reference their response to LabMD's request that they produce "[a]ll 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."

56. Indeed, Complaint Counsel even objected to LabMD's interrogatory inquiring what "data-security standards, regulations, and guidelines the FTC will use to determine whether LabMD's data-security practices were not reasonable and appropriate" on the ground that it seeks opinions by undisclosed nontestifying experts and "calls for expert opinions."

57. The thousands of pages of materials that FTC enforcement staff have produced to LabMD in response to the foregoing document request (most of which was produced on March 3, 2014, two days before the close of fact discovery) consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of

FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. Some of these materials are of very recent vintage and dated after the events described in the FTC's August 2013 administrative complaint allegedly occurred. Some of these materials are dated after August 28, 2013, when the FTC issued this complaint. The only regulations that FTC enforcement staff produced to LabMD do not apply to LabMD and implement statutes that also do not apply to LabMD.

58. On March 3, 2014, FTC enforcement staff refused to admit, among other things, that the FTC's administrative complaint does not specifically reference any industry standards for data-security practices, hardware or software necessary to avoid a violation of Section 5, instead claiming that LabMD was asking for "an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside of the scope of discovery" and, in the alternative, denying that they were required to allege this.

59. FTC enforcement staff have even argued that "STANDARDS USED TO ENFORCE SECTION 5 ARE OUTSIDE THE SCOPE OF DISCOVERY," saying that "[t]he orders and opinions of the Commission and of th[e ALJ] ...

preclude such discovery.” Complaint Counsel’s Motion for Protective Order Regarding Rule 3.33 Notice of Deposition, *In the Matter of LabMD*, FTC Dkt. No. 9357, at 7 (Feb. 14, 2014).

60. More recently, on March 18, 2014, FTC enforcement staff produced an expert witness report that for the first time—after more than four years of investigation and litigation—gave LabMD some notice as to what a FTC expert thinks LabMD did wrong. But that report did not even purport to assess LabMD’s PHI data-security practices against any objective, applicable medical-industry data-security statute, regulation, custom, or standard.

III. LabMD Challenges The FTC’s Jurisdiction.

61. On November 12, 2013, LabMD filed a dispositive Motion to Dismiss raising pure issues of law and questions of statutory interpretation in the FTC’s administrative case. A true and correct copy is attached hereto as Exhibit 11. LabMD requested oral argument. Under the FTC’s Rules of Practice, Commissioners (and not the ALJ) rule on dispositive motions to dismiss complaints they recently voted to issue in the first instance.

62. On November 14, 2014, LabMD also filed a Verified Complaint in the U.S. District Court for the District of Columbia seeking solely injunctive and

declaratory relief. LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 1 (D.D.C. Nov. 14, 2013).

63. On November 18, 2013, LabMD filed a petition for review in the U.S. Court of Appeals for the Eleventh Circuit, LabMD, Inc. v. FTC, Case No. 13-14267-F (11th Cir. Nov. 18, 2013). Ex. 1.

64. On November 25, 2013, LabMD filed an administrative stay motion in the FTC enforcement action.

65. On December 2, 2013, LabMD filed a reply in support of its administrative motion to dismiss. A true and correct copy is attached hereto as Exhibit 12.

66. On December 13, 2013, the FTC issued an order denying LabMD's stay motion ("December 13 Order"). A true and correct copy is attached hereto as Exhibit 13. The December 13 Order states that no Article III court has jurisdiction over LabMD's claims until the FTC gives its permission.

67. On December 16, 2013, the Eleventh Circuit issued two jurisdictional questions to the parties. Jurisdictional Questions, LabMD v. FTC, Case No. 13-15267-F (Dec. 16, 2013).

68. On December 23, 2013, LabMD filed a stay motion in in the Eleventh Circuit. Petitioner’s Motion for Stay Pending Review, LabMD v. FTC, Case No. 13-15267-F (Dec. 23, 2013).

69. On January 16, 2014, the FTC denied LabMD’s administrative Motion to Dismiss, rejecting LabMD’s jurisdictional and fair-notice due process challenges without oral argument, thereby denying LabMD an opportunity to create a record (the “January 16 Order”). Ex. 2.

70. On January 17, 2014, the FTC submitted the January 16 Order to the Eleventh Circuit, via what it called a “notice of supplemental authority.”

71. FTC did the exact same thing on the exact same day in FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-SCM, Dkt. No. 151 (D. N.J. Jan. 17, 2014). The FTC claimed its order had the force of law and should be given deference under “Chevron.” Ex. 3 at 6.

72. The FTC admits that it cannot and does not enforce HIPAA or HITECH. Ex. 2 at 12 & n.19.

73. The FTC admits that its case against LabMD solely alleges statutory Section 5 statutory “unfairness” violations, not “violations of the FTC’s Health Breach Notification Rule.” Id. at 20 n.20.

74. The FTC admits that it has failed to establish any data-security standards with the force of law that give notice as to what PHI data-security practices the Commission and its enforcement staff believes Section 5 forbids or requires. Ex. 2 at 15.

75. The FTC admits that it did not claim data-security regulatory authority until years after 1994, when Section 5 was last amended to add subsection (n). 15 U.S.C. § 45(n). Ex. 2 at 4, 8-9. Subsection (n) does not mention “data security,” let alone explain what data-security practices the FTC believes Section 5 to forbid or require.

76. Yet the FTC claims subsection (n) gives fair notice: “Here, the three-part statutory standard governing whether an act or practice is ‘unfair,’ set forth in Section 5(n) [15 U.S.C. § 45], should dispel LabMD’s concern about whether the statutory prohibition of ‘unfair . . . acts or practices’ is sufficient to give fair notice of what conduct is prohibited.” Ex. 2 at 16.

77. The FTC’s January 16 Order essentially asserts that constitutional fair-notice due process requirements are somehow inapplicable here because, according to the Defendant, the FTC is not pursuing “criminal punishment or civil penalties for past conduct.” Ex. 2 at 16.

78. The FTC also claims it is not obligated to provide any fair notice at all of the PHI data-security practices it believes Section 5 to forbid or require because agencies have broad “discretion” to “address an issue by rulemaking or adjudication.” Ex. 2 at 15.

79. For that matter, the FTC effectively claims that the standard for Section 5 “unfairness” PHI data-security liability is whether a company’s practices are “unreasonable” according to it, while acknowledging that this is a case of first impression as to what is “unreasonable.”

80. Elsewhere, the FTC admitted that there is no process through which businesses could have obtained guidance or an advisory opinion from the Commission regarding data-security practices. See Hearing Trans., FTC v. Wyndham et al., Case No. 2:13-cv-01887-ES-SCM, 52:10-11 (Nov. 7, 2012). A true and correct copy of an excerpt of the foregoing transcript is attached hereto as Exhibit 14 and is incorporated herein by reference.

81. On February 18, 2014, the Eleventh Circuit dismissed LabMD’s Petition for Review and denied all pending motions as moot because there was no cease and desist order reviewable under 15 U.S.C. § 45(c). Instead, it ruled this Court has original jurisdiction over LabMD’s ultra vires, statutory, and constitutional claims to

the extent that such claims could be asserted before a cease and desist order is entered.

Ex. 1.

82. Therefore, on February 19, 2014, LabMD filed a Notice of Voluntary Dismissal Without Prejudice of LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 20 (D.D.C.), because under D.C. Circuit law, which is different from the law of this Circuit, only the U.S. Court of Appeals for the D.C. Circuit has jurisdiction over those claims, yet the D.C. Circuit will never have jurisdiction under 15 U.S.C. § 45(c) because LabMD has not done business there.

83. The FTC has issued a final agency decision regarding jurisdiction, and LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional fair-notice due process arguments.

IV. The FTC Denies LabMD Procedural Due Process.

84. To begin with, the FTC has never specified the PHI data-security standards LabMD failed to meet, thereby denying LabMD an opportunity to effectively defend itself and granting the Commission, Mr. Sheer, and other federal bureaucrats unlimited discretion to decide what is “unreasonable” after the fact and to regulate the entire health care industry based on their idiosyncratic whim, caprice, and fancy.

85. In 2009, the FTC modified its Rules of Practice to deny respondents a fair defense and to render motion practice futile. 74 Fed. Reg. 20,205 (May 1, 2009).

86. At the initial pretrial conference, the ALJ told LabMD's counsel:

[L]et me talk about dispositive motions There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you. Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission

Ex. 9 at 18:11-15. The ALJ lacks power to even grant a continuance of the evidentiary hearing or stay the proceedings pending adjudication of dispositive motions before the Commission. See 16 C.F.R. §§ 3.22(b), 3.41(b).

87. The FTC was extensively warned about the constitutional implications of its power-grab during the comment period.

88. The American Bar Association (ABA) Section of Antitrust Law ("Antitrust Section") said the revisions forced respondents to address prehearing issues to the FTC without the benefit of a prior opinion authored by a party who was not involved in crafting and approving a complaint. Comments of the ABA Section of Antitrust Law in Response to the Federal Trade Commission's Request for Public Comment Regarding Parts 3 and 4 Rules of Practice Rulemaking—P072194, at 4 (Nov. 6, 2008).

89. The Antitrust Section explained that its “primary concern is that by ‘codifying’ the Commission’s right to interject itself into prehearing case management, it may undermine the integrity of the process, compromise the ALJ, and create an appearance of unfairness.” Id. at 12. The Antitrust Section also said the FTC’s amendments “could reduce the quality of decision making, and may color the perception of the fairness and impartiality of Commission proceedings—a particularly important issue considering that when hearing an appeal, federal courts will give deference to a final FTC decision.” Id. at 11.

90. The U.S. Chamber of Commerce added that “it appears that the proposed changes are being rushed into place and for the purpose of giving the FTC material, tactical, and procedural advantage” U.S. Chamber of Commerce, Comment, Re: Parts 3 and 4 Rules of Practice Rulemaking—P072104, at 1 (Nov. 6, 2008). In fact:

The FTC’s proposed regulations work to effectively eliminate the role of the independent Administrative Law Judge (ALJ) to manage and prepare an initial decision for a case. This results in the elimination of a vital check on potential unfairness inherent in the FTC’s administrative procedure. Under the FTC’s process, the Commissioners act as both prosecutor and judge in administrative trials. Thus, the same individuals who decide to issue the complaint also decide the final appeal of the administrative trial. With such a clear potential for unfairness or conflict of interest at the forefront of FTC administrative adjudication, it is necessary to preserve some sort of fairness check.

Id. at 2.

91. Under current Commission Rule 3.22(a), “[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision shall be directly referred to the Commission and shall be ruled on by the Commission unless the Commission in its discretion refers the motion to the Administrative Law Judge.”

92. In excess of their authority and in violation of the Constitution’s guarantee of due process, the FTC has assumed for itself the power to legislate, to prosecute, and to judge LabMD without even specifying in advance the elements of the data-security offense LabMD has allegedly committed.

93. The empirical evidence demonstrates that the FTC’s administrative process is a rigged exercise in futility for LabMD and others similarly situated.

94. According to Commissioner Wright:

The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges (“ALJs”) in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed.

Joshua D. Wright, Comm’r, Fed. Trade Comm., Recalibrating Section 5: A Response to the CPI Symposium, CPI Antitrust Symposium, at 4 (November 2013), available at

http://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf (last visited Mar. 18, 2014).

95. Further administrative proceedings are exhausted and futile.

V. The Irreparable Harm Done By The FTC To LabMD.

96. FTC's power-grab has destroyed LabMD's customer relationships and, in large measure, driven LabMD to cease accepting new specimen samples. But for all of the time, attention, and money LabMD has been forced to devote to addressing the FTC's actions, the company would almost certainly be accepting new specimen samples and providing cancer-diagnostic services to doctors to this day.

97. LabMD, and its doctors, have been denied insurance coverage as a direct result of the FTC's ongoing persecution of the company. For example, One Beacon (a medical malpractice insurance company) recently denied LabMD, and its doctors, coverage, saying: "[W]e are unable to offer ERP terms for the entity [LabMD], and as a result, the individual physicians so I will be closing the file. The potential volatility due to the FTC investigation is something we want to stay away from particularly because it pertains to medical records."

98. LabMD's general liability insurance carrier is planning to non-renew its insurance policy effective May 6, 2014.

99. The FTC's personnel have intentionally interfered with LabMD's customer relationships and effectively engaged in a campaign of commercial disparagement.

100. The FTC's actions have caused, and continue to cause, irreparable injury to LabMD's business reputation and good will in the marketplace.

101. The FTC, Mr. Sheer, and other FTC employees have intentionally set out to destroy LabMD's commercial brand, reputation, and good will.

102. The FTC, Mr. Sheer, and others have caused and continue to cause LabMD irreparable harm far beyond mere litigation expenses and threaten the viability of LabMD's business operations. Much of this harm cannot be quantified in monetary terms, and cannot be remedied by monetary damages. For example, on January 6, 2014, LabMD notified its customers that it would no longer be accepting new specimen samples for testing for the foreseeable future, effective January 11, 2014.

CLAIMS FOR RELIEF

First Claim for Relief (For Violation of the APA)

103. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 54-61, 64-66, 69-81, 84, and 93-95.

104. The FTC's action against LabMD is arbitrary, capricious, an abuse of discretion and power, in excess of statutory authority and short of statutory right, and contrary to law and constitutional right, in violation of 5 U.S.C. § 706.

105. The FTC does not have jurisdiction to regulate LabMD's patient-information data-security and thus its actions are ultra vires.

106. The Commission's orders denying the jurisdictional, ultra vires, and due process claims raised in LabMD's motion to dismiss and LabMD's motion for a stay are both "final agency actions" within the meaning of 5 U.S.C. § 704 and thus LabMD's APA claims are ripe and reviewable now. TVA v. Whitman, 336 F.3d 1236, 1248 (11th Cir. 2004); see, e.g., CSI Aviation Servs. v. DOT, 637 F.3d 408, 411-14 (D.C. Cir. 2011); see Sackett, 132 S. Ct. at 1371-72; see also Athlone Indus., Inc. v. CPSC, 707 F.2d 1485, 1487-88 (D.C. Cir. 1983).

107. LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional due-process arguments, which the Commission formally rejected on January 16, 2014.

108. In addition, only administrative remedies providing a genuine opportunity for adequate relief need be exhausted, and here exhaustion is also independently not required because the administrative process is futile and inadequate and LabMD will continue to suffer irreparable harm unless its claims are reviewed by

an Article III Court now. See N.B. by D.G. v. Alachua Cnty. Sch. Bd., 84 F.3d 1376, 1379 (11th Cir. 1996); Porter v. Schweiker, 692 F.2d 740, 742-43 (11th Cir. 1982); Randolph-Sheppard Vendors of Am. v. Weinberger, 795 F.2d 90, 107-08 (D.C. Cir. 1986) (irreparable harm excuses exhaustion).

109. Therefore, the FTC's enforcement action against LabMD should be enjoined and a declaration issued that it lacks authority to regulate patient information data-security.

Second Claim for Relief
(For Ultra Vires Agency Action)

110. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 61, 70-81, and 93-96.

111. Regardless of the presence vel non of "final agency action" under 5 U.S.C. § 704, this Court has jurisdiction to adjudicate LabMD's nonstatutory ultra vires and constitutional claims, for the presence or absence of "final agency action" has no jurisdictional effect. See, e.g., Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006); Muniz-Muniz v. U.S. Border Patrol, No. 12-4419, 2013 U.S. App. LEXIS 25400, at *11 (6th Cir. Dec. 20, 2013) (noting that "all of our sister circuits" have concluded 5 U.S.C. § 704 has no effect on a federal-question jurisdiction to adjudicate non-APA claims); see also Arbaugh v. Y & H Corp., 546 U.S. 500, 511, 516-17 (2006).

112. Thus, the FTC's ultra vires actions are ripe for judicial review now regardless of the reviewability of LabMD's APA claims.

113. Exhaustion is not required for these claims under any circumstances. See XYZ Law Firm v. FTC, 525 F. Supp. 1235, 1237 (N.D. Ga. 1981).

114. The FTC's actions against LabMD exceed the power given to it in Section 5 and are thus ultra vires.

115. Judicial review of this claim is available because the Defendant's ultra vires actions exceed the authority conferred on it by Congress and the United States Constitution.

116. Moreover, inter alia, the FTC has effectively violated three specific and mandatory restraints on its Section 5 "unfairness" power.

117. First, the FTC's abuse exceeds its delegated powers and is contrary to specific the FTC Act's prohibitions on the use of consent orders and speeches to create a binding "common law" of data security. 15 U.S.C. § 45(m)(1)(B).

118. Second, in addition to the fact that Congress has not given the FTC Section 5 "unfairness" authority to regulate data security, let alone authority to over-file HHS and regulate PHI data security, the FTC has also independently violated 15 U.S.C. § 45(n)'s specific limits on its Section 5 "unfairness" authority. 15 U.S.C. § 45(n) explicitly states that the Defendant "shall have no authority under this section

or section 18 [15 U.S.C. § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair” under the circumstances of this case. 15 U.S.C. § 45(n) further explicitly bars the FTC from using its public policy views as a primary basis for exercising its unfairness authority.

119. Third, the FTC’s sworn responses to LabMD’s discovery requests demonstrate it is seeking to enforce against LabMD random Internet postings, e-mail alerts, Commission staff reports, and congressional testimony they say establish data-security standards LabMD should have followed, even those these documents do not have the force of law and were not even published in the Federal Register, and they do not allege that LabMD had actual knowledge of any of these Internet postings and other materials. 5 U.S.C. § 552(a)(1).

120. FTC’s unauthorized actions are the direct and proximate cause of LabMD’s injuries, as described above. Therefore, LabMD is entitled to the declaratory and injunctive relief requested herein.

Third Claim for Relief
(For Fair-Notice Due Process Violations)

121. LabMD repeats paragraphs 4-5, 7-10, 46-49, 74-80, 84-85, and 118-119.

122. This Court has jurisdiction over LabMD’s fair-notice due process claim now. Exhaustion is not required for these claims under any circumstances.

123. The Fifth Amendment to the United States Constitution states that “[n]o person shall be . . . deprived of life, liberty, or property, without due process of law.” U.S. Const. amend. V.

124. The draft notice order (“Commission Notice Order”) if made effective, will be in place for twenty (20) years and, inter alia, require LabMD to (1) “establish and implement, and thereafter maintain, a . . . security program”; (2) “obtain initial and biennial assessment and reports” from third parties for a period of twenty (20) years; (3) provide Commission-approved notice to the individuals listed in the accounts-receivable file and their health insurance companies of Tiversa’s actions via first-class mail; (4) deliver copies of the Commission Notice Order to “current and future principals, officers, directors, and managers,” as well as deliver copies to many current and future employees, agents, representatives, and business entities; (5) notify the FTC in writing at least thirty (30) days before making numerous changes, such as change in corporate name or address; and (6) prepare and file detailed reports with the FTC.

125. Additionally, the FTC has reserved the right to order such other relief as it finds necessary and appropriate if it decides that the Commission Notice Order is insufficient, including seeking “restitution” and other types of relief authorized by Section 19 of the Federal Trade Commission Act, 15 U.S.C. § 57b (civil actions for

violations of rules and cease and desist orders respecting unfair or deceptive acts or practices), including but not limited to rescission or reformation of contracts and payment of monetary damages.

126. Under 15 U.S.C. § 45(l), each violation of the FTC cease and desist orders carries up to a \$10,000 civil penalty.

127. FTC's actions, January 16 Order, December 13 Order, and the Commission Complaint and Notice Order, thus implicate LabMD's property rights, which are protected by the Due Process Clause of the Fifth Amendment.

128. FTC's refusal to promulgate any regulations or to issue any other guidelines clarifying and providing any notice, let alone constitutionally adequate notice, of what data-security practices they believe Section 5 forbids or requires, or to otherwise establish any meaningful standards, violates LabMD's due process rights.

129. Due process requires that laws that regulate persons or entities must give fair notice of conduct that is forbidden or required. FCC v. Fox TV Stations, Inc., 132 S. Ct. 2307, 2317 (2012); Connally v. Gen. Constr. Co., 269 U.S. 385, 391-95 (1926).

130. This constitutional fair-notice requirement has been thoroughly incorporated into administrative law to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. Georgia Pac. Corp. v. OSHRC, 25 F.3d 999, 1005 (11th Cir. 1994). Fair-notice due process requirements thus apply to the

FTC administrative enforcement actions seeking to impose cease and desist orders for alleged violations of Section 5.

131. The FTC has failed to meet its burden of establishing reasonably ascertainable standards for what data-security practices it believes Section 5 to either forbid or to require. See Georgia Pac. Corp., 25 F.3d at 1005; Trinity Broad. of Fla., Inc. v. FCC, 211 F.3d 618, 628-32 (D.C. Cir. 2000).

132. Basic principles of due process limit the FTC's "discretion" to enforce Section 5 through administrative adjudications; specifically, the FTC can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires. The FTC has failed to provide LabMD the baseline level of fair notice of the data-security practices it believes to be required or forbidden by Section 5's "unfairness" language.

133. Because the FTC's Section 5 PHI data-security regulatory scheme forbids or requires the doing of an act in terms so vague that men and women of common intelligence must necessarily guess at its meaning and differ as to its application, it violates due process.

134. In addition, even if the FTC's "reasonableness" standard for PHI data security otherwise passed constitutional muster, the FTC's failure to link its data-security standards to medical-industry standards independently violates due process.

135. FTC's pattern and practice of fair-notice due process violations, as applied to LabMD and all similarly situated, including the defendants in FTC v. Wyndham, violates due process.

Fourth Claim for Relief

(For Facial, Structural Due Process Violations)

136. LabMD repeats paragraphs 4-5, 7-10, 17-19, 23-34, and 84-96.

137. Exhaustion of administrative remedies is not required for facial and structural due process challenges. See, e.g., Matthews v. Eldridge, 424 U.S. 319, 329-32 (1976); Amos Treat & Co. v. SEC, 306 F.2d 260, 267 (D.C. Cir. 1963).

138. The substantial private interests affected by the FTC's actions, the high risk of erroneous deprivation of LabMD's property interests, and the high value of additional procedural safeguards outweigh the FTC's de minimis interest in the existing procedures. Therefore, LabMD has not been provided the procedural safeguards that it is constitutionally entitled to have.

139. Due process minimally requires a fair trial in a fair tribunal and "this applies to administrative agencies which adjudicate as well as to courts." Withrow v. Larkin, 421 U.S. 35, 46-47 (1975).

140. FTC's modifications to its Rules of Practices transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions and deprive

all respondents of a fair administrative hearing. Therefore, the Commission's Rules facially and structurally violate due process.

141. Furthermore, the FTC's ex post facto enforcement action against LabMD for alleged violations of unspecified data-security standards in a proceeding in which the FTC acts in a legislative, prosecutorial, and adjudicative capacity further violates due process.

142. Finally, the FTC has predetermined this matter, denying LabMD its right to a fair and level review, including a fair hearing on its Motion to Dismiss before an impartial ALJ.

143. FTC's intentional violations of LabMD's due process rights has caused LabMD hundreds of thousands of dollars in actual damages, harmed its business reputation, caused it to lose good will and business opportunities, and brought the company to the brink of ruin.

Fifth Claim for Relief

(For Retaliation Against LabMD for Protected First Amendment Speech)

144. LabMD repeats paragraphs 4-5, 7-11, 23-49, and 53.

145. The First Amendment to the United States Constitution guarantees LabMD freedom of speech.

146. Mr. Daugherty's book, his webpage about the book, and his speeches and statements about the FTC's actions are political speech and speech about matters of public concern and thus protected by the First Amendment.

147. On information and belief, the FTC's actions against LabMD were retaliation for protected speech by Mr. Daugherty.

148. The FTC's actions against LabMD, as set forth herein, will likely chill a person of ordinary firmness from engaging in the protected First Amendment activity.

149. On information and belief, the FTC's conduct herein was precisely intended and designed, at least in part, to punish LabMD and chill government criticism by LabMD and others targeted by the government.

150. Even if the FTC, Complaint Counsel, and other FTC employees disagree with and find Mr. Daugherty's statements about their actions to be patently offensive, they are not allowed retaliate by bringing an enforcement action against LabMD.

RELIEF REQUESTED

WHEREFORE LabMD requests the following relief:

A. That the Court enter a declaratory judgment that (1) the FTC lacks statutory authority to regulate patient-information data-security practices under Section 5; (2) the FTC's efforts to regulate patient information are ultra vires; (3) the FTC violated LabMD's due process rights by failing to provide constitutionally

adequate notice of what data-security practices the Commission believed Section 5 to forbid or require before the Complaint was filed; (4) the FTC violated LabMD's due process rights by unconstitutionally combining legislative, prosecutorial, investigative, and adjudicatory functions by, among other things, allowing FTC Commissioners to rule on dispositive motions concerning complaints they recently voted to issue; and (5) the FTC unconstitutionally retaliated against LabMD for engaging in constitutionally protected speech.

B. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall take no further actions in connection with administrative proceedings known as In the Matter of LabMD, FTC Dkt. No. 9357, including but not limited to issuing orders, holding hearings, taking discovery, and filing motions.

C. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall not (1) initiate any civil or administrative enforcement action against LabMD or any other person on the ground that their patient information data-security practices are "unfair" in violation of Section 5; (2) investigate whether LabMD's or any other person's patient

information data-security practices violate Section 5 for “unfairness”; (3) attempt to establish substantive data-security standards under Section 5 and/or enforce Section 5 in civil or administrative proceedings; or (4) undertake or pursue any administrative enforcement proceedings until the Commission amends its Rules of Practice to provide constitutionally adequate due process.

D. That the Court award LabMD its attorneys’ fees and litigation costs under the Equal Access to Justice Act and/or such other applicable law.

E. Such other and further relief as this Court deems just and proper.

Respectfully submitted, this 20th day of March, 2014.

KILPATRICK TOWNSEND
& STOCKTON LLP
1100 Peachtree Street, NE
Suite 2800
Atlanta, Georgia 30309
Telephone (404) 815-6500
Facsimile (404) 815-6555
rraider@kilpatricktownsend.com
bsingleton@kilpatricktownsend.com
bmeyer@kilpatricktownsend.com

/s/ Ronald L. Raider
Ronald L. Raider
Georgia Bar No. 592192
Burleigh L. Singleton
Georgia Bar No. 649084
William D. Meyer
Georgia Bar No. 950008

Counsel for Plaintiff

OF COUNSEL:

Reed D. Rubinstein
(applying for admission pro hac vice)
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
reed.rubinstein@dinsmore.com

Senior Vice President for Litigation and
Counsel to Cause of Action

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

Dated: March 20, 2014

Verification

I am Michael Daugherty, owner and CEO of LabMD, Inc., which is the plaintiff in this action.

I have read the foregoing Complaint and verify and declare on behalf of LabMD, Inc., under penalty of perjury, that its factual allegations are true, except to those matters stated on information and belief, and as to those matters I believe them to be true to the best of my knowledge.

LabMD, Inc.

By:


Michael Daugherty

Date:

3/19/14

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14 point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: March 20, 2014.

/s/ Ronald L. Raider
Ronald L. Raider

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

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

NOTICE OF APPEAL

Notice is hereby given that LabMD, Inc., Plaintiff in the above-named case, hereby appeals to the United States Court of Appeals for the Eleventh Circuit from the Order granting the Defendant, Federal Trade Commission's ("FTC") Motion to Dismiss the Complaint, DE 33, entered in this action on May 12, 2014, and the Judgment entered in favor of the FTC, DE 34, on May 12, 2014.

Respectfully submitted, this 14th day of May, 2014.

KILPATRICK TOWNSEND
& STOCKTON LLP
1100 Peachtree Street, NE
Suite 2800
Atlanta, Georgia 30309
Telephone: (404) 815-6500
Facsimile: (404) 815-6555
rraider@kilpatricktownsend.com
bsingleton@kilpatricktownsend.com
bmeyer@kilpatricktownsend.com

/s/ Burleigh L. Singleton

Ronald L. Raider
Georgia Bar No. 592192
Burleigh L. Singleton
Georgia Bar No. 649084
William D. Meyer
Georgia Bar No. 950008

Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Telephone: (202) 499-4232
Facsimile: (202) 330-5842
michael.pepson@causeofaction.org

/s/ Michael D. Pepson

Michael D. Pepson
(admitted *pro hac vice*)

Admitted only in Maryland.
Practice limited to federal matters.

DINSMORE & SHOHL, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: (202) 372-9120
Facsimile: (202) 372-9141
reed.rubinstein@dinsmore.com

Reed D. Rubinstein
(admitted *pro hac vice*)
D.C. Bar No. 440153

Senior Vice President for Litigation and
Counsel to Cause of Action

Counsel for Plaintiff

CERTIFICATION AS TO FONT

In accordance with Local Rule 7.1(D), the undersigned certifies that this brief was prepared with Times New Roman 14, a font and point selection approved by the Court in Local Rule 5.1.

/s/Burleigh L. Singleton

Counsel for Plaintiff

CERTIFICATE OF SERVICE

This is to certify that, on May 14, 2014, undersigned hereby certifies that a true and correct copy of the foregoing has been filed with the U.S. District Court's CM/ECF System and that pursuant thereto, a copy of the **NOTICE OF APPEAL** has been served upon the following persons by electronic mail:

Lauren E. Fascett, Esq.
Perham Gorji, Esq.
Trial Attorneys
U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street NW
Washington, DC 20001
lauren.fascett@usdoj.gov
perham.gorji@usdoj.gov

This 14th day of May, 2014.

/s/ Burleigh L. Singleton
Counsel for Plaintiff

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

LabMD, Inc.,

Plaintiff,

vs.

Federal Trade Commission,

Defendant.

CIVIL ACTION FILE

NO. 1:14-cv-810-WSD

J U D G M E N T

This action having come before the court, Honorable William S. Duffey, Jr., United States District Judge, for consideration of Defendant's Motion to Dismiss, and the court having granted said motion, it is

Ordered and Adjudged that the action be, and the same hereby, is **dismissed**.

Dated at Atlanta, Georgia, this 12th day of May, 2014.

JAMES N. HATTEN
CLERK OF COURT

By: s/ Ashley Coleman
Deputy Clerk

Prepared, Filed, and Entered
in the Clerk's Office
May 13, 2014
James N. Hatten
Clerk of Court

By: s/ A. Coleman
Deputy Clerk

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

LabMD, Inc.

Plaintiff,

v.

1:14-cv-00810-WSD

FEDERAL TRADE COMMISSION,

Defendant.

OPINION AND ORDER

This matter is before the Court on LabMD's ("Plaintiff") Motion for Preliminary Injunction [2] and the Federal Trade Commission's ("Defendant" or "FTC") Motion to Dismiss the Plaintiff's Complaint [13]. A hearing on the Motion for Preliminary Injunction was conducted on May 7, 2014.

I. BACKGROUND

A. Factual and Procedural History

Plaintiff is a small medical laboratory based in Atlanta, GA, that provided doctors with cancer-detection services. In January, 2010, the Defendant commenced an investigation into the Plaintiff's data security practices regarding

Protected Health Information (“PHI”)¹ based upon the claim that sensitive information in the Plaintiff’s possession and control had been disclosed by means of a peer-to-peer file sharing network available to the public. Three and a half years later, the Defendant issued an Administrative Complaint against the Plaintiff in which it alleged that there was “reason to believe” that Plaintiff may have engaged in “unfair . . . acts or practices,” under 15 U.S.C. § 45(a)(1) of the Federal Trade Commission Act (“Section 5”), because Plaintiff failed to provide reasonably adequate security for patient information retained on its internal network. The Administrative Complaint also alleged that Plaintiff had the capacity to prevent the vulnerabilities in its data security infrastructure “at relatively low cost using readily available security measures,” and that the ultimate consumers allegedly harmed due to the Plaintiff’s lax data security were unable to protect themselves because they “ha[d] no way of independently knowing” about the alleged disclosures. Def.’s Mot. to Dismiss and Resp. to Pl.’s Mot. for Prelim. Inj. at 7.

The Administrative Complaint cited two specific examples of alleged data

¹ PHI refers to individually identifiable health information, including the individual’s name, social security number, address, birth date, history of mental and physical health condition, provision of health care, and payment history for the provision of health care.

security failures at LabMD. First, that LabMD failed to discover that its billing manager had installed a peer-to-peer file sharing application known as Limewire on his or her work computer, and a file that contained personal information on approximately 9,300 consumers was accessible to any individual, who used or had access to Limewire's software. Second, that the police department in Sacramento, California arrested alleged identity thieves, and found, in their possession, LabMD's documents containing sensitive pertinent personal information on individuals.²

On November 12, 2013, Plaintiff moved the Commission to dismiss the Administrative Complaint on the grounds that the FTC had no statutory authority to address the data security practices of private companies under Section 5, and that the application of Section 5 to LabMD's data security practices violated the Due Process Clause of the United States Constitution. On January 16, 2014, the Commission denied the Plaintiff's Motion to Dismiss, concluding that Section 5 vests the FTC with authority to address a private company's data security practices "as unfair . . . acts or practices" if they are found to be so deficient that it "causes

² At the May 7, 2014, Preliminary Injunction hearing, the FTC informed the Court that it was unaware whether the alleged identity thieves arrested in Sacramento received documents containing PHI as a consequence of LabMD's data security failures.

or is likely to cause substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [the harm is] not outweighed by countervailing benefits to consumers or competition.” 15 U.S.C. § 45(n). The Commission also found that the Administrative Complaint sufficiently stated a claim that the Plaintiff engaged in “unfair . . . acts or practices” because of its alleged failure to maintain adequate data security, and stressed that the “ultimate decision on LabMD’s liability will depend on the factual evidence to be adduced in this administrative proceeding.” Pl.’s Ex. 3 at 18.

The claims alleged in the Administrative Complaint have been referred to an administrative law judge (“ALJ”) in the underlying adjudicatory proceeding. On May 20, 2014, the ALJ will conduct an evidentiary hearing to determine whether the Plaintiff’s data security practices violated Section 5. After the ALJ issues an initial decision, either party may appeal to the Commission for *de novo* review of the ALJ’s factual findings and legal conclusions. 5 U.S.C. § 557(b). If the Commission concludes that the Plaintiff engaged in “unfair . . . acts or practices,” and enters a cease and desist order, the Plaintiff has a statutory right to “obtain a review of such order in the court of appeals.” 15 U.S.C. § 45(c).

On November 14, 2013, the Plaintiff filed a complaint against the FTC in the United States District Court for the District of Columbia, seeking to enjoin the

enforcement action on the grounds that (1) the FTC abused its statutory authority by regulating LabMD's data security practices, (2) the FTC's application of Section 5 to LabMD's data security practices violated the Due Process Clause, and (3) the FTC brought the enforcement action to retaliate against LabMD's President's public criticism of the agency. On December 23, 2013, the Plaintiff filed in the Eleventh Circuit a Motion to Stay the administrative proceedings, arguing that a stay was necessary to prevent irreparable harm, including on the grounds that the FTC's application of Section 5 to LabMD's data security practices lacked statutory authority, and the FTC's actions were *ultra vires* and unconstitutional. On February 18, 2014, the Eleventh Circuit, *sua sponte*, dismissed the Plaintiff's petition for lack of jurisdiction.

The Eleventh Circuit concluded that its authority, under § 45(c), did not extend beyond review of a final cease and desist order. The Eleventh Circuit, however, "[did] not express or imply any opinion about whether a district court has jurisdiction to hear [the plaintiff's] claims or about the merits of those claims."

On February 19, 2014, the Plaintiff voluntarily dismissed its complaint pending before the United States District Court for the District of Columbia. A month later, the Plaintiff filed a Verified Complaint ("Complaint") for Declaratory and Injunctive relief in this Court. The Complaint alleges that (1) the FTC action

is arbitrary and capricious under the Administrative Procedures Act (“APA”) because the FTC does not have the statutory authority to regulate PHI under Section 5; (2) the FTC action is an *ultra vires* act that exceeds its congressional and constitutional authority; and (3) the FTC’s application of Section 5 to LabMD’s data security practices violates the requirements of fair notice, and the right to a fair hearing in a fair tribunal under the Due Process Clause of the United States Constitution. The Complaint also alleges that the FTC violated LabMD’s First Amendment right to free speech by filing the Administrative Complaint. On March 20, 2014, Plaintiff filed a Motion for Preliminary Injunction to enjoin the ongoing administrative proceeding before the ALJ, and to enjoin the FTC from asserting any further data security actions against LabMD.

At the core, LabMD’s claims in this matter are identical to those filed in the United States District Court for the District of Columbia and the Eleventh Circuit. LabMD alleges that Section 5 does not authorize an action for alleged security breaches involving PHI that is not provided to LabMD by patients but by physicians ordering laboratory tests for their patients. It claims also that PHI is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, which discredits that the FTC has the authority to

regulate data security under Section 5. LabMD further alleges that the FTC has not published any requirements for the protection of patient information, and thus LabMD is not on notice of what protections the FTC now claims were required. LabMD claims that the FTC brought its enforcement action against LabMD to retaliate against its President's public criticism of the FTC, which were published through the press, social media, and in a book entitled *The Devil Inside the Beltway: The Shocking Expose of the US Government's Surveillance and Overreach into Cybersecurity, Medicine and Small Business*.³

On April 7, 2014, the FTC replied to LabMD's Motion for Preliminary Injunction, and moved under Rule 12(b)(1) of the Federal Rules of Civil Procedure to dismiss the Complaint for lack of jurisdiction and moved under Rule 12(b)(6) to dismiss for failure to state a claim. On April 11, 2014, LabMD filed its Response in Opposition to the FTC's Motion to Dismiss. On April 16, 2014, the FTC replied to LabMD's Response to its Motion to Dismiss the Complaint.

³ At the May 7, 2014 hearing, Mr. Daugherty testified that FTC employees accessed his blog 75 times shortly after he criticized the FTC for bringing an enforcement action against LabMD. Preliminary Injunction Hr'g Tr., May 7, 2014, at 23: 9-20. Counsel for the FTC did not know why FTC personnel repeatedly accessed Mr. Daugherty's blog shortly after the criticisms were published, but surmised that a possible explanation for accessing the blog was that FTC personnel wanted to ensure that Mr. Daugherty's free speech rights were not impeded. *Id.* at 24-28.

II. DISCUSSION

A. Legal Standard

1. *Motion to Dismiss*

The law governing motions to dismiss pursuant to Rule 12(b)(6) is well-settled. Dismissal of a complaint is appropriate “when, on the basis of a dispositive issue of law, no construction of the factual allegations will support the cause of action.” Marshall Cnty. Bd. of Educ. v. Marshall Cnty. Gas Dist., 992 F.2d 1171, 1174 (11th Cir. 1993).

In considering a motion to dismiss, the Court accepts the plaintiff’s allegations as true and considers the allegations in the complaint in the light most favorable to the plaintiff. See Hishon v. King & Spalding, 467 U.S. 69, 73 (1984); Watts v. Fla. Int’l Univ., 495 F.3d 1289, 1295 (11th Cir. 2007); see also Bryant v. Avado Brands, Inc., 187 F.3d 1271, 1273 n.1 (11th Cir. 1999) (“At the motion to dismiss stage, all well-pleaded facts are accepted as true, and the reasonable inferences therefrom are construed in the light most favorable to the plaintiff.”). The Court, however, is not required to accept a plaintiff’s legal conclusions. See Sinaltrainal v. Coca-Cola Co., 578 F.3d 1252, 1260 (11th Cir. 2009) (citing Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)), abrogated on other grounds by Mohamad v. Palestinian Auth., 132 S. Ct. 1702 (2012). The Court also will not

“accept as true a legal conclusion couched as a factual allegation.” See Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007). Ultimately, the complaint is required to contain “enough facts to state a claim to relief that is plausible on its face.” Twombly, 550 U.S. at 570.⁴

To state a claim to relief that is plausible, the plaintiff must plead factual content that “allows the Court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Iqbal, 556 U.S. at 678. “Plausibility” requires more than a “sheer possibility that a defendant has acted unlawfully,” and a complaint that alleges facts that are “merely consistent with” liability “stops short of the line between possibility and plausibility of ‘entitlement to relief.’” Id. (citing Twombly, 550 U.S. at 557). “To survive a motion to dismiss, plaintiffs must do more than merely state legal conclusions; they are required to allege some specific factual bases for those conclusions or face dismissal of their claims.”

Jackson v. BellSouth Telecomms., 372 F.3d 1250, 1263 (11th Cir. 2004)

(“[C]onclusory allegations, unwarranted deductions of facts or legal conclusions

⁴ The Supreme Court explicitly rejected its earlier formulation for the Rule 12(b)(6) pleading standard: “[T]he accepted rule [is] that a complaint should not be dismissed for failure to state a claim unless it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief.” Twombly, 550 U.S. at 577 (quoting Conley v. Gibson, 355 U.S. 41, 45-46 (1957)). The Court decided that “this famous observation has earned its retirement.” Id. at 563.

masquerading as facts will not prevent dismissal.”) (citations omitted).⁵

B. Analysis

Under § 704 of the APA, “[a]gency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review.” 5 U.S.C. § 704. “The requirement of a final agency action has been considered jurisdictional. If the agency action is not final, the court therefore cannot reach the merits of the dispute.” Nat’l Parks Conservation Ass’n v. Norton, 324 F.3d 1229, 1236 (11th Cir. 2003) (internal citations and quotation marks omitted). An agency action is considered final when two requirements are met: (1) the action marks the “consummation of the agency’s decisionmaking process”—it must not be of a tentative or interlocutory nature, and (2) the action must be one by which “rights or obligations have been determined” or from which “legal consequences will flow.” Bennett v. Spear, 520 U.S. 154, 177-78 (1994). A non-final agency action is one that “does not itself adversely affect the complainant but only affects his rights adversely on the contingency of

⁵ Federal Rule of Civil Procedure 8(a)(2) requires the plaintiff to state “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). In Twombly, the Supreme Court recognized the liberal minimal standards imposed by Federal Rule 8(a)(2) but also acknowledged that “[f]actual allegations must be enough to raise a right to relief above the speculative level” Twombly, 550 U.S. at 555.

future administrative action.” Rochester Tel. Corp. v. United States, 307 U.S. 125, 130 (1939).

LabMD contends that the Commission’s interlocutory decision to deny its Motion to Dismiss the Administrative Complaint is a final agency action because the Commission has concluded that Section 5 allows the FTC to regulate PHI retained by medical service providers, and, that the FTC is authorized to impose obligations on those providers who maintain PHI even if it supplements the requirements of other federal statutes. LabMD also argues that the FTC has treated the Commission’s Order as a final agency action because the FTC submitted the Order to the Eleventh Circuit and the District Court of New Jersey as supplemental legal authority, requesting those courts to afford Chevron deference to the Commission’s interpretation of Section 5.

While the Eleventh Circuit has not directly addressed the issue, those courts that have universally hold that a direct attack on the agency’s statutory or constitutional authority to conduct an investigation or commence an enforcement action does not allow a plaintiff to evade administrative review or avoid administrative procedures. Aluminum Co. of America v. United States, 790 F.2d 938, 942 (D.C. Cir. 1986) (observing that a claim attacking an agency’s assertion of jurisdiction as beyond statutory authority does not make a difference to the

finality analysis because the purpose of finality is to prevent piecemeal “consideration of rulings that may fade into insignificance by the time the initial decisionmaker disassociates itself from the matter.”); see also VeldHoen v. United States Coast Guard, T.A., 35 F.3d 222 (5th Cir. 1994); Dairymen, Inc. v. FTC, 684 F.2d 376, 378-79 (6th Cir. 1982).

The Commission’s denial of LabMD’s Motion to Dismiss the Administrative Complaint on the grounds that the FTC does not have the statutory authority to regulate data security practices under Section 5 is the type of Order that “ha[s] long been considered nonfinal.” DRG Funding Corp. v. Secretary of HUD, 76 F.3d 1212, 1215 (D.C. Cir. 1996). The Commission’s Order is the equivalent of a district court’s decision to deny a motion to dismiss, “which—unlike a final order ending the case—assures its continuation.” Id. LabMD’s contention that the Commission’s interlocutory Order is a final agency action because it concluded that the FTC has statutory authority to regulate PHI under Section 5 has specifically been rejected by other courts.

In American Airlines Inc. v. Herman, for example, the plaintiff argued that it would be “futile for it to pursue the administrative process because the DOL already has finally and definitively rejected each of [the] challenges to its statutory and regulatory authority.” 176 F.3d 283, 292 (5th Cir. 1999). The Fifth Circuit

rejected the plaintiff's argument, and held that "the requirement that the reviewable order be definitive in its impact on the rights of the parties is something more than a requirement that the order be unambiguous in legal effect. It is a requirement that the order have some substantial effect *which cannot be altered by subsequent administrative action.*" Id. (internal quotation marks and citations omitted) (emphasis in original). Because of the possibility that the plaintiff could prevail on the merits in the administrative proceeding, the Fifth Circuit required the plaintiff to submit to the administrative proceeding. Id.

The Court concludes that it does not have jurisdiction over this action because even if it determines that the Commission's position on the FTC's authority to regulate PHI under Section 5 was definitive, the mere assertion of jurisdiction does not impose or fix an obligation on LabMD from which "legal consequences may flow." Bennett, 520 U.S. at 177-78. The Commission's denial of LabMD's Motion to Dismiss the Administrative Complaint is not a final agency action, and the FTC's decision to submit the Commission's Order to other courts as "supplemental authority" is a litigation tactic that does not render final a Commission Order that is not. The possibility that LabMD may prevail on the merits if the ALJ, or the Commission, concludes that it did not violate Section 5 will moot its judicial challenge and render it unnecessary for the Court to intervene

in an ongoing administrative proceeding.⁶ American Airlines Inc., 176 F.3d at 292. See also FTC v. Standard Oil Co. of California, 449 U.S. 232, 242 (1980) (observing that “judicial intervention into the agency process denies the agency an opportunity to correct its own mistakes and to apply its expertise,” and that “intervention also leads to piecemeal review which at the least is inefficient and upon completion of the agency process might prove to have been unnecessary.”) (citations omitted).

LabMD alleges that the burdens imposed by the FTC investigation and the requirement to submit to an administrative proceeding crippled its day to day business because it had to effectively shut down its operations, lay off more than two dozen employees, and cannot procure medical malpractice and property insurance to remain a going concern. Even if the Court accepts these allegations as true, the expense and burdens associated with complying with an agency’s information requests and submitting to an administrative proceeding do not qualify as legally recognized harms, and do not provide a basis upon which to grant

⁶ The Court believes that the likelihood of a favorable jurisdictional or merits outcome for LabMD is slight, but that belief cannot govern the legal issues addressed in this Order. As the Court noted at the May 7, 2014 hearing, the authority of the FTC to enlarge its regulatory activity in the data security area presents an interesting and likely important jurisdictional issue that needs to be resolved promptly.

LabMD relief. Standard Oil Co. of California, 449 U.S. at 244 (“litigation expense, even substantial and unrecoupable cost, does not constitute irreparable injury” because “the expense and annoyance of litigation is part of the social burden of living under government.”) (internal citations and quotation marks omitted); see also Imperial Carpet Mills, Inc. v. Consumer Prod. Safety Comm’n, 634 F.2d 871, 874 (5th Cir. Unit B Jan. 1981)⁷ (holding that “the burden of defending against the Complaint; the expense of complying with the Commission’s anticipated final order; the resulting bad publicity; and the potential for a dangerous loss of credit” do not justify intervention into administrative agency action).⁸

⁷ In Bonner v. City of Prichard, the Eleventh Circuit adopted as binding precedent decisions of the Fifth Circuit handed down prior to October 1, 1981. 661 F.2d 1206, 1209-10 (11th Cir. 1981).

⁸ LabMD’s claim that the FTC investigation had a crippling effect on its business is questionable in light of Mr. Daugherty’s testimony at the Preliminary Injunction hearing. In 2010, the FTC began its investigation into LabMD’s data security practices. Four years later, in January, 2014, LabMD decided to no longer provide cancer detection services, which is the essence of its business operations. Preliminary Injunction Hr’g Tr., at 6: 20-25. LabMD continued to operate as a going concern throughout the FTC investigation until the end of 2013. In 2013, LabMD retained 25 to 30 employees on its payroll, and it continued to generate a profit margin of approximately 25% until 2013 when the company experienced a loss of half a million dollars. Id. at 11: 1-25. The company “never had problems getting insurance prior to 2013.” Id. at 12: 6-8. The evidence presented at the Preliminary Injunction hearing demonstrates that an insurer’s decision to deny tail risk coverage to LabMD on account of the FTC investigation and administrative

LabMD's view that the Court can address and review its constitutional claims based on the Due Process Clause and the First Amendment regardless of whether there is a final agency action under the APA is contrary to established precedent. In Ticor Tile Ins. Co. v. FTC, the plaintiff mounted a facial challenge to the constitutionality of Section 5, arguing that the FTC had definitively concluded that the provision was constitutional, and that the FTC's position constituted final agency action reviewable in a federal court before the consummation of the administrative proceeding. 814 F.2d 731, 738-743, 746-749 (D.C. Cir. 1987). The D.C. Circuit affirmed the dismissal of plaintiff's complaint because there was no final agency action, the plaintiff did not exhaust its remedies in the administrative proceeding, and the case was not ripe for review. Id. at 732; Id. at 748 (Williams, J.) (explaining that even if unconstitutional actions are accepted as "heavier" than "those of statutory illegality, the constitutional dimension of appellants' burden entails a concern that militates powerfully against

proceeding was not made until January 13, 2014, which is a week after LabMD had decided to discontinue its cancer detection services. See Pl.'s Ex. 15, attached to Pl.'s Ex. List. At the Preliminary Injunction hearing, Mr. Daugherty, conceded that the implementation of the Affordable Care Act, and its resulting effect on cost containment and market consolidation negatively impacted LabMD's operations, and "creat[ed] huge anxiety, destruction, consolidation in our customer base." Id. at 52: 9-21. Mr. Daugherty also conceded that LabMD's future "depend[ed] on Obamacare, and other than that I don't know." Id. at 54: 1-4.

immediate review: the fundamental rule of judicial restraint, forbidding resolution of constitutional questions before it is necessary to decide them.”) (internal citations and quotation marks omitted).

In the absence of final agency action, LabMD’s alleged constitutional injuries are not currently ripe for review. North Carolina State Bd. of Dental Examiners v. FTC, 768 F. Supp. 2d 818, 824 (E.D.N.C 2011) (holding that in the absence of a final cease and desist order from the Commission, plaintiff has failed to show that its constitutional rights have been or are being violated); see also E. I. Dupont de Nemours and Co. v. FTC, 488 F. Supp. 747, 754 (D. Del. 1980) (rejecting the plaintiff’s claim that the FTC violated its First Amendment rights by filing a complaint because the FTC did not direct the plaintiff to stop engaging in speech, and there was no indication that significant costs or sanctions on the use of protected expression would be imposed on the plaintiff to stifle its free speech as the “only ‘threat’ that is involved in the administrative proceedings is the threat that a cease and desist order will be issued [and] . . . no other sanctions or penalties can be imposed . . . as the result of those proceedings.”).

Finally, LabMD asserts that even if the Commission’s Order regarding its jurisdiction does not constitute final agency action, the Leedom exception applies, allowing the Court to review LabMD’s constitutional and *ultra vires* claims.

Under the Leedom exception, federal courts typically lack jurisdiction to enjoin an ongoing administrative proceeding, Ewing v. Mytinger & Casselberry, Inc., 339 U.S. 594, 598 (1950), unless the agency commits an “egregious error” that plainly violates an unambiguous and mandatory provision of a federal statute, and the aggrieved party has no adequate or meaningful opportunity to vindicate its rights. Leedom v. Kyne, 358 U.S. 184 (1958); American Airlines Inc., 176 F.3d at 293-94. The Court concludes that the Leedom exception does not apply here because the FTC’s application of Section 5 to the data security practices of private companies is not contrary to an unambiguous and mandatory provision of a federal statute. In American Airlines Inc., the Fifth Circuit specifically held that the Leedom exception does not apply to a “dispute over whether an agency charged with a statute’s implementation has interpreted it correctly.” 176 F.3d at 293. That is the crux of the Plaintiff’s Complaint in this matter, but it is insufficient to invoke the exception under Leedom. LabMD can obtain meaningful and adequate review of its jurisdictional challenge in the Court of Appeals, if that is necessary.


III. CONCLUSION

Accordingly, for the foregoing reasons,

IT IS HEREBY ORDERED that the Defendant’s Motion to Dismiss the Complaint for lack of jurisdiction is **GRANTED** [13].

IT IS FURTHER ORDERED that the Plaintiff's Motion for Preliminary Injunction is **DENIED AS MOOT** [2].

SO ORDERED this 12th day of May 2014.



WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE

**UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT**

ELBERT PARR TUTTLE COURT OF APPEALS BUILDING
56 Forsyth Street, N.W.
Atlanta, Georgia 30303

John Ley
Clerk of Court

For rules and forms visit
www.ca11.uscourts.gov

May 15, 2014

William D. Meyer
Kilpatrick Townsend & Stockton, LLP
1100 PEACHTREE ST STE 2800
ATLANTA, GA 30309

Michael David Pepson
Cause of Action
1919 PENNSYLVANIA AVE NW STE 650
WASHINGTON, DC 20006

Ronald Lee Raider
Kilpatrick Townsend & Stockton, LLP
1100 PEACHTREE ST STE 2800
ATLANTA, GA 30309

Reed Darrow Rubinstein
Dinsmore & Shohl, LLP
801 PENNSYLVANIA AVE NW STE 610
WASHINGTON, DC 20004

Burleigh Lavisky Singleton
Kilpatrick Townsend & Stockton, LLP
1100 PEACHTREE ST STE 2800
ATLANTA, GA 30309

Appeal Number: 14-12144-EE
Case Style: LabMD, Inc. v. Federal Trade Commission
District Court Docket No: 1:14-cv-00810-WSD

This Court requires all counsel to file documents electronically using the Electronic Case Files ("ECF") system, unless exempted for good cause.

The referenced case has been docketed in this court. Please use the appellate docket number noted above when making inquiries.

Eleventh Circuit Rule 31-1 requires that APPELLANT'S BRIEF BE SERVED AND FILED ON OR BEFORE **June 24, 2014**. APPELLANT'S APPENDIX MUST BE SERVED AND FILED NO

LATER THAN 7 DAYS AFTER FILING OF THE APPELLANT'S BRIEF.

This is the only notice you will receive concerning the due date for filing briefs and appendices. See Fed.R.App.P. 28, 30, 31, 32, the corresponding circuit rules, General Order 39 and the Guide to Electronic Filing for further information. Pro se parties who are incarcerated are not required to file an appendix. (In cross-appeals pursuant to Fed.R.App.P. 28(h), the party who first files a notice of appeal is the appellant unless the parties otherwise agree.)

FRAP 26.1 and the accompanying circuit rules provide that the Certificate of Interested Persons and Corporate Disclosure Statement (CIP) must be filed with the court by every appellant, appellee, intervenor and amicus curiae, including governmental parties. Appellants (and cross-appellants) must file their CIP within 14 days of the date this appeal has been docketed, or along with the filing in this court of any motion, petition, or pleading, whichever occurs first. The time for filing the opposing party's CIP or notice is set by 11th Cir. R. 26.1-2(c). On the same day the CIP is served, the party filing it must also complete the court's web-based certificate at the Web-Based CIP link of the court's website. Pro se parties are **not required or authorized** to complete the web-based certificate.

Attorneys who wish to participate in this appeal must be properly admitted either to the bar of this court or for this particular proceeding pursuant to 11th Cir. R. 46-1. In addition, all attorneys (except court-appointed counsel) who wish to participate in this appeal must complete and return an appearance form within fourteen (14) days. Application for Admission to the Bar and Appearance of Counsel Form are available on the Internet at www.ca11.uscourts.gov. The clerk may not process filings from an attorney until that attorney files an appearance form. See 11th Cir. R. 46-6.

11th Cir. R. 33-1(a) requires appellant to file a Civil Appeal Statement in most civil appeals. You must file a completed Civil Appeal Statement, with service on all other parties, within 14 days from the date of this letter. Civil Appeal Statement forms are available on the Internet at www.ca11.uscourts.gov, and as provided by 11th Cir. R. 33-1(a).

MEDIATION. If a Civil Appeal Statement is required to be filed, your appeal and all related matters will be considered for mediation by the Kinnard Mediation Center. The mediation services are free and the mediation process is confidential. You may confidentially request mediation by calling the Kinnard Mediation Center at 404-335-6260 (Atlanta) or 305-714-1900 (Miami). See 11th Cir. R. 33-1.

Sincerely,

JOHN LEY, Clerk of Court

Reply to: Lois Tunstall, EE
Phone #: (404) 335-6224

DKT-7CIV Civil Early Briefing

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.

A handwritten signature in blue ink that reads "Donald S. Clark" with a long horizontal line extending to the right.

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.

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

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

ONE HUNDRED THIRTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

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

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.").

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.*

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) 225-6000
FACSIMILE (202) 225-5001

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.

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Monday, November 17, 2014 11:47 AM
To: White, Christian S.
Subject: VM: VanDruff, Laura Riposo (2999)
Attachments: Voice_Message_Recording_S1296941_001_gsm.wav

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



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

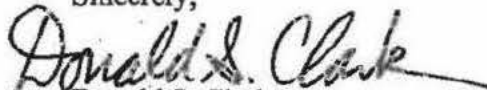
June 13, 2014

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

WAI TELL E ISSA CALIFORNIA
CHAIRMAN

JOHN L. BROWN, OHIO
WILHELM H. BURGER, OHIO
JOHN J. DINGELL, MICHIGAN
PATRICK J. SCHUMER, NEW YORK
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMMIE FRANKFORD, OKLAHOMA
JUSTIN SMITH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICIA MULLIN, PENNSYLVANIA
SCOTT LEE BARRON, TENNESSEE
TERRY ADAMS, SOUTH CAROLINA
BLAKE FLETCHER, TEXAS
DODD HASTINGS, WASHINGTON
CYNTHIA L. LUMM, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DUSTY COBB, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. CONRAD, MICHIGAN
RON DEWANE, LOUISIANA

KENNETH J. BLOOM
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

MASTERY (202) 225-6766
FACSIMILE (202) 225-3874
TELEPHONE (202) 225-2081
http://oversight.house.gov

June 11, 2014

ELIJAH F. CUMMINGS, MARYLAND
RANKING MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. FLEGGY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPECTER, PENNSYLVANIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROHM L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORNBERG, NEVADA
MICHELLE LUMMAN GOSHAM, NEW MEXICO
WAGNER

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,

A handwritten signature in dark 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

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

COA # 000097
FTC-FOIA-2015-00109

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 -----

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

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

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

Duplicate

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

COA # 000103
FTC-FOIA-2015-00109

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 tivversa..

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

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

ONE HUNDRED THIRTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

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

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.").

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.*

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) 225-6000
FACSIMILE: (202) 225-5001

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.

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; Hipsley, 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

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

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Thursday, November 06, 2014 12:50 PM
To: White, Christian S.
Subject: thank you!

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

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

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

June 17, 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

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.

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, Mr. 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?

⁶ Boback Tr. at 129.

⁷ *Id.*

⁸ *Id.* at 129-130.

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.

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/>.

Ms. Kelly Tshibaka
June 17, 2014
Page 4

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,

A handwritten signature in blue ink, appearing to read "Darrell Issa", with a large, stylized flourish extending to the right.

Darrell Issa
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCENRY, 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

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.*

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.

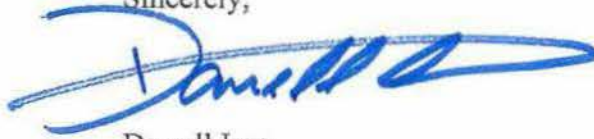
The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony 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: 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.

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

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



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

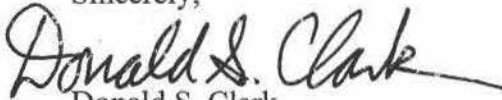
June 13, 2014

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

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL B. 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

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. HORNFORD, 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.*

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.

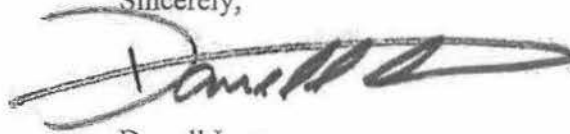
The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony 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". The signature is stylized with a large, sweeping initial "D" and a long horizontal stroke extending to the right.

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: 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

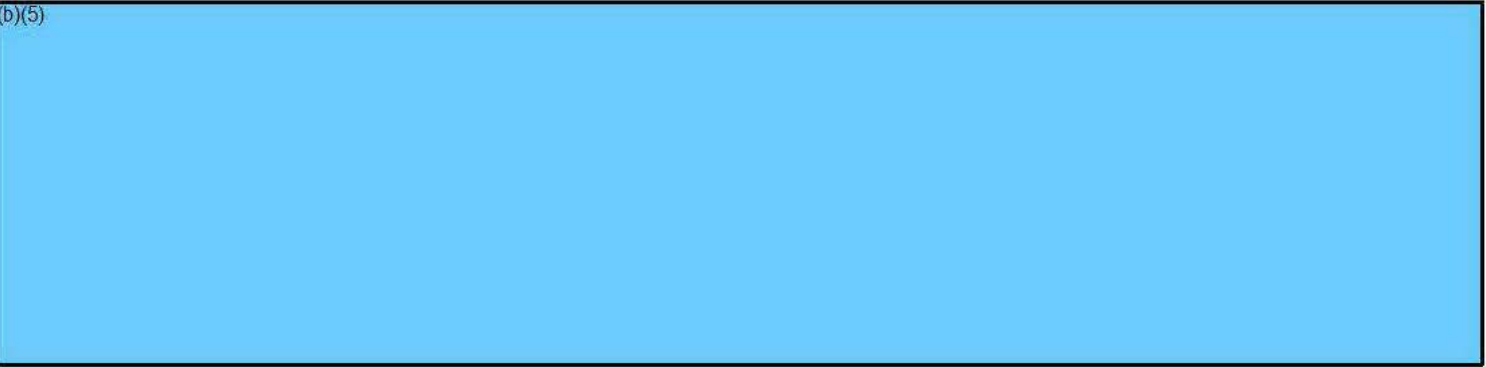
Looks good to me Don.

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

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.

Duplicate

COA # 000135
FTC-FOIA-2015-00109

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



United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

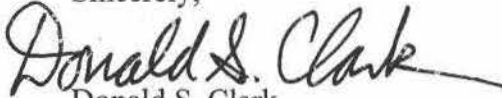
June 13, 2014

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

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL B. 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

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.*

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.

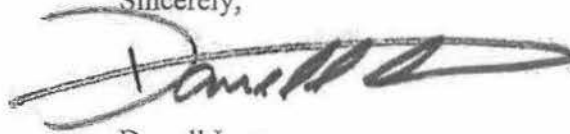
The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony 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". The signature is stylized with a large, sweeping initial "D" and a long horizontal stroke extending to the right.

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: 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.

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)

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)

(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

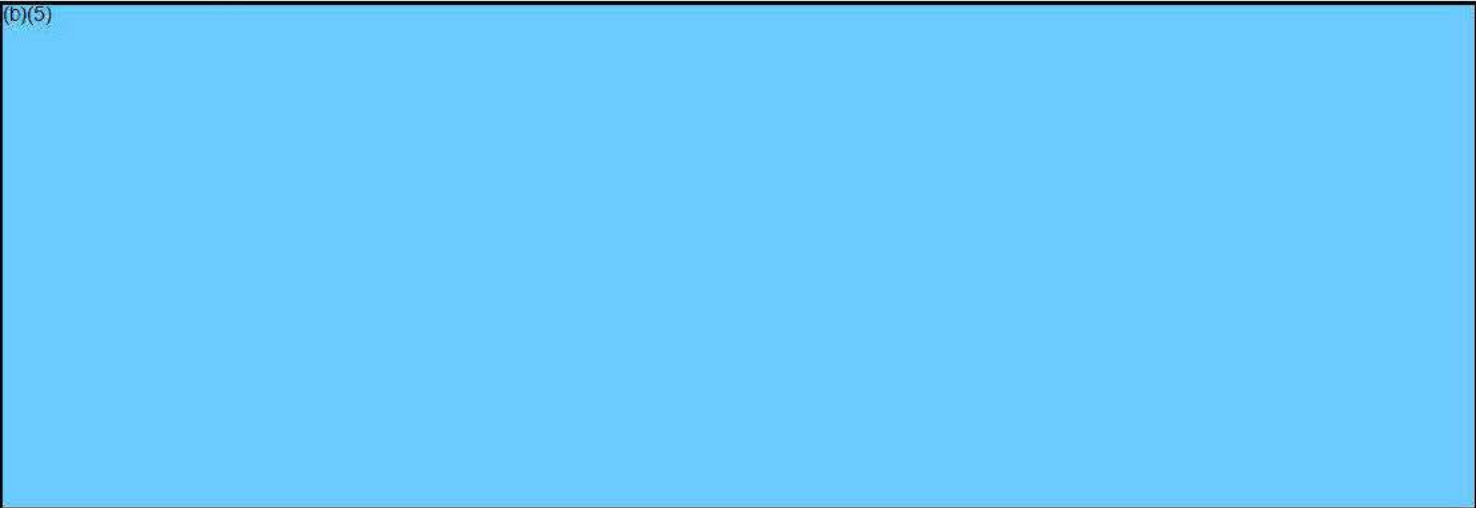
Importance: High

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

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>

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.*

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.

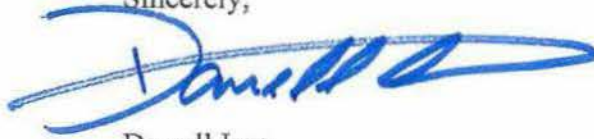
The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony 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 blue ink, appearing to read "Darrell Issa", with a large, sweeping flourish extending to the right.

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

Kelly, Andrea

From: Sheer, Alain
Sent: Tuesday, June 10, 2014 2:18 PM
To: White, Christian S.
Subject: RE: (b)(5) Thanks. Alain

Thanks Chris

From: White, Christian S.
Sent: Tuesday, June 10, 2014 2:17 PM
To: Sheer, Alain
Subject: RE: (b)(5) Thanks. Alain

From: Sheer, Alain
Sent: Tuesday, June 10, 2014 2:15 PM
To: White, Christian S.
Subject: (b)(5) 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,

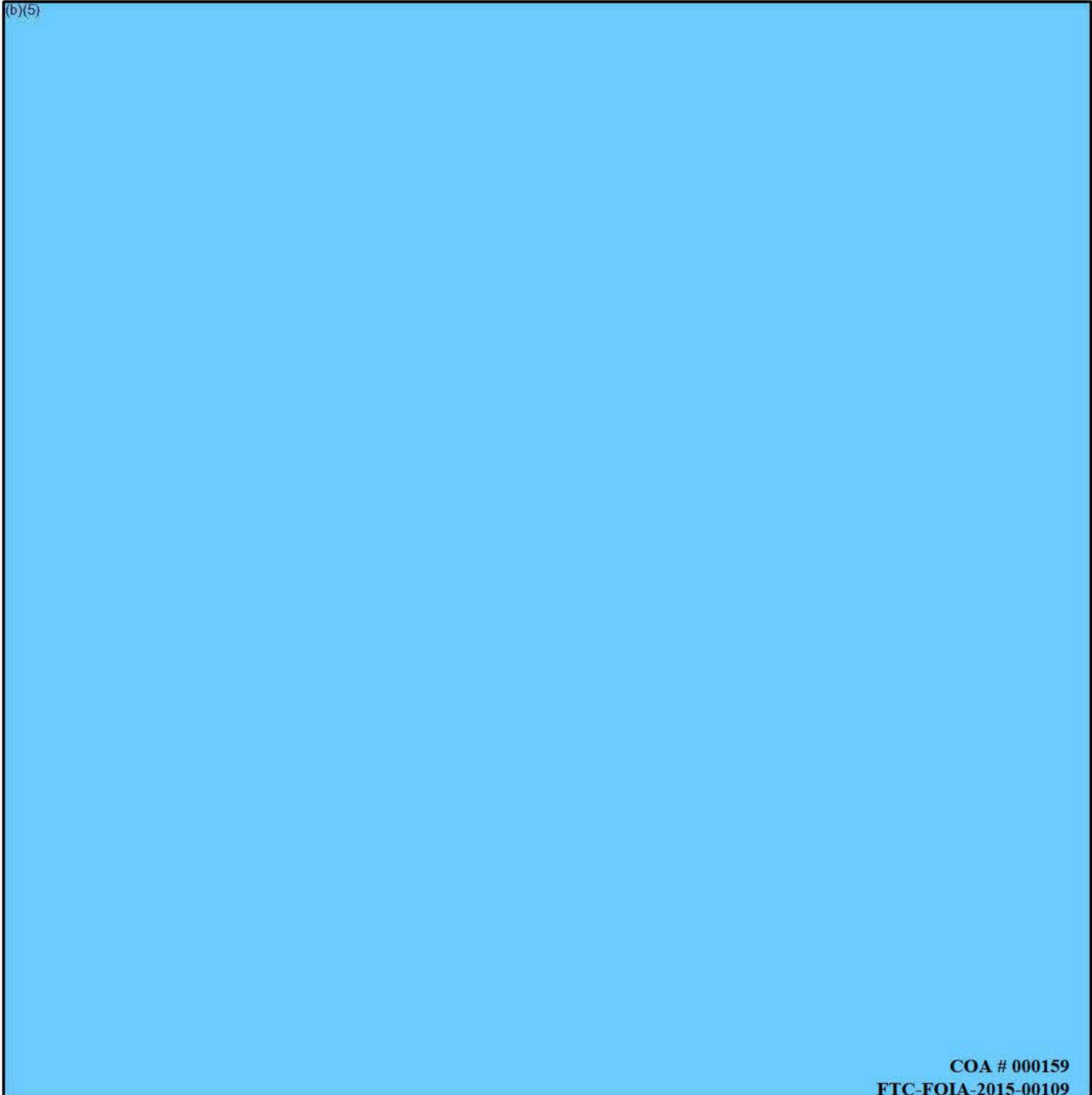
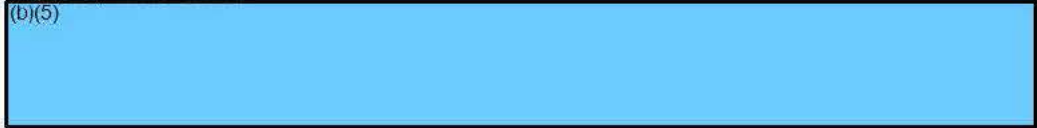
Laura

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

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Wednesday, November 05, 2014 10:46 AM
To: White, Christian S.
Subject: (b)(5)

Attachments:



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

Kelly, Andrea

From: Sheer, Alain
Sent: Monday, June 02, 2014 9:21 AM
To: White, Christian S.
Subject: RE:

Hi Chris. (b)(5) [Redacted]
(b)(5) [Redacted] 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) [Redacted] H
(b)(5),(b)(6) [Redacted]

Kelly, Andrea

From: Schoshinski, Robert
Sent: Thursday, April 03, 2014 4:30 PM
To: White, Christian S.
Subject: FW: new brief from DOJ
Attachments: LabMD PI Oppn4-2DOJ.docx

Chris:

(b)(5)



Thanks,

Bob Schoshinski

(b)(5)



COA # 000162
FTC-FOIA-2015-00109

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)

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)

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

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Thursday, March 13, 2014 4:59 PM
To: White, Christian S.
Subject: VM: VanDruff, Laura Riposo (2999)
Attachments: Voice_Message_Recording_S1121540_001_gsm.wav

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)

ORIGINAL

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



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

DOCKET NO. 9357

**ORDER DENYING RESPONDENT'S
MOTION FOR A RULE 3.36 SUBPOENA**

On January 30, 2014, Respondent filed a Motion for a Rule 3.36 Subpoena to require the production of documents that are in the possession, custody, or control of the FTC Commissioners or the FTC's Office of Public Affairs ("Motion"). Complaint Counsel filed its opposition on February 10, 2014 ("Opposition").

Having fully reviewed the Motion and the Opposition, and having considered all arguments and contentions raised therein, the Motion is DENIED, as explained below.

I. Introduction

The Complaint charges that Respondent, a lab that provides doctors with cancer detection services, engaged in an unfair trade practice in violation of Section 5(a) of the FTC Act by failing to take reasonable and appropriate measures to prevent unauthorized access to consumers' personal information. Complaint ¶¶ 6-11, 17-21, 23. Allegations of the Complaint relevant to the Motion are:

- 1) one of LabMD's files containing confidential patient information ("the 1718 file") was accessible through a public peer-to-peer ("P2P") file sharing network; Complaint ¶¶ 10(g), 17-20;
- 2) 35 LabMD "Day Sheets,"¹ containing confidential patient information, and a small number of copied checks were found in the possession of individuals who subsequently pleaded no contest to state charges of identity theft ("the Sacramento Incident"); Complaint ¶ 21; and

¹ As alleged in the Complaint, Day Sheets are spreadsheets of payments received from consumers, which may include personal information such as consumer names, Social Security Numbers, and methods, amounts, and dates of payments. Complaint ¶ 9.

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

Kelly, Andrea

From: VanDruff, Laura Riposo
Sent: Monday, November 03, 2014 5:07 PM
To: White, Christian S.
Subject: RE: VM: VanDruff, Laura Riposo (2999)

Absolutely. Feel better, Chris.

-----Original Message-----

From: White, Christian S.
Sent: Monday, November 03, 2014 4:58 PM
To: VanDruff, Laura Riposo
Subject: Re: VM: VanDruff, Laura Riposo (2999)

I'm out sick. Can I call you tomorrow?

----- Original Message -----

From: VanDruff, Laura Riposo
Sent: Monday, November 03, 2014 04:22 PM
To: White, Christian S.
Subject: VM: VanDruff, Laura Riposo (2999)

Kelly, Andrea

From: Federal Trade Commission <subscribe@subscribe.ftc.gov>
Sent: Wednesday, January 29, 2014 8:41 AM
To: White, Christian S.
Subject: Daily Clips 01.29.14

**Federal Trade
Commission**

Protecting
America's
Consumers



DAILY CLIPS

January 29, 2014 (Wednesday)

COMPETITION

FTC Says Cephalon Put Ex-GC's Advice In Play. [Law360](#) 1/28 (pasted below)

FTC clears way for Kroger, Harris Teeter deal. [Daily Press](#) 1/28 (blog)

Smith seeks FTC review of propane prices. [The Salem News](#) 1/28

Life Technologies acquisition to clear FTC this week. [Daily Deal](#) 1/28

Falling Gasoline Hurts Exxon Plea for U.S. Crude Exports. [Bloomberg](#) 1/28

Frozen Northeast Getting Gouged by Natural Gas Prices. [Businessweek](#) 1/28

California Gas Prices Fall 8 Cents In Last 2 Weeks. [AP](#) (via CBS Local) 1/27

CONSUMER PROTECTION

FTC Cyber Case Has Nearly Put Us Out of Business, Firm Says. [WSJ](#) 1/28 (pasted below)

LabMD Winding Down Operations, Blaming FTC Suit. [Law360](#) 1/28 (pasted below)

FTC rules HIPAA not a barrier to security enforcement. [Fierce Health IT](#) 1/28

FTC Staff Expresses Support for a Shift in Bank Monitoring Rules. [LoanSafe](#) 1/28

Video: FTC Says Nissan Frontier Commercial is Misleading. [Auto Evolution](#) 11/29 (blog)

FTC's 'Net Cetera' Advises Parents on How to Talk to Their Kids . [Yumanewsnow](#) 1/28

Video: \$9.84 charge a red flag. [USAT](#) 1/29

Cybercrooks use stolen consumer data hour-to-hour. [USAT](#) 1/28

DMA Prepping New Data Breach Protection Guidelines. [Broadcasting & Cable](#) 1/28

3 Steps to Take After a Data Breach. [Fox Business](#) 1/28

Personal Finance: Important lessons from the Target data breach. [Chattanooga Times Free Press](#) 1/29

Delamaide: Financial watchdog digs in. [USAT](#) 1/28

FTC Slaps Diaper Company for False Biodegradability Claims. [Environmental Leader](#) 1/27

OF INTEREST

Exclusive: Google close to settling EU antitrust investigation – sources. [Reuters](#) 1/29

No more Sunday ad supplements -- unless you subscribe. [Market Place](#) 1/28

Higher rates loom for some modified mortgages. [USAT](#) 1/29

COMPETITION LAW 360

FTC Says Cephalon Put Ex-GC's Advice In Play

By Melissa Lipman

Jan 28 2014

The Federal Trade Commission argued Monday in Pennsylvania federal court that Cephalon Inc. had put the testimony of its former general counsel at issue in the antitrust watchdog's pay-for-delay suit, saying the company should either be compelled to turn over the materials or blocked from using them at trial.

The agency accused Cephalon of twisting the position the FTC took in a motion to compel in order to skirt the real question at issue in the dispute.

"Cephalon's opposition to the FTC's motion to compel is little more than an effort to ignore the elephant in the room," the agency said. "The elephant here ... is Cephalon's use of the testimony of its former general counsel."

The FTC, which sued Cephalon in 2008 alleging that the drugmaker paid off would-be competitors to prevent generic versions of their narcolepsy drug Provigil from making it to market, took issue in December with Cephalon's plans to use evidence of its views about the strength of the underlying patent as a key part of its defense to the FTC's case.

Cephalon had maintained that the merits of its underlying patent infringement case against several generic rivals were irrelevant to the antitrust case, but in November the company for the first time argued that "'evidence about the perceived strength of the patent at the time of settlement' is both relevant and potentially 'critical' to a rule of reason analysis of its conduct," the FTC said in its original filing.

To that end, the company offered a statement from its former general counsel in support of its bid to keep the FTC from successfully barring the company from making those kinds of arguments at trial, according to the FTC filing.

But Cephalon hit back at that request and similar motions to compel brought by the private plaintiffs in mid-January, saying it had long "zealously guarded" its attorney client

privilege in the case.

"As this court has previously recognized in denying plaintiffs' essentially indistinguishable prior privilege motions, the fact that a party's state of mind may be relevant does not mean that legal advice is "at issue" and the privilege has been waived," Cephalon wrote at the time.

But the FTC maintains that Cephalon strategically quoted from its motion in order to "fundamentally distort" what the FTC actually said.

"The issue presented by the FTC's motion to compel is whether, given the context and circumstances, Cephalon's use of its attorney's testimony as a material element of its defense against the FTC's charges is an 'affirmative step' that has put the advice of Cephalon's counsel at issue," the FTC wrote.

While Cephalon's filing implied that the testimony from its former general counsel relates only to the private plaintiffs' case, the FTC noted that Cephalon never said in its filing that it would not use that same testimony to defend itself in the FTC case.

A spokesman for the FTC declined to comment on the matter.

An attorney for Cephalon wasn't immediately available for comment Tuesday.

Cephalon is represented by James C. Burling, Peter A. Spaeth and Mark Ford of WilmerHale and John A. Guernsey and Nancy J. Gellman of Conrad O'Brien PC.

The case is Federal Trade Commission v. Cephalon Inc., case number 2:08-cv-02141, in the U.S. District Court for the Eastern District of Pennsylvania.

THE WALL STREET JOURNAL

FTC Cyber Case Has Nearly Put Us Out of Business, Firm Says

By Rachel Louise Ensign

Jan 28 2014

A firm battling the Federal Trade Commission's authority to regulate its corporate cybersecurity said it has stopped most of its operations because of costs tied to the agency's case.

Medical testing laboratory LabMD Inc. stopped collecting new specimens earlier this month, according to a letter to customers filed in federal court as part of its dispute with the agency. The firm is also now "closed for phone calls and Internet access" though reports and billing are still available, the letter said.

"This action is in large part due to the conduct of the Federal Trade Commission," President and Chief Executive Michael J. Daugherty wrote in the letter. "The FTC has subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient-information data-security vulnerability."

The privately held Atlanta firm has shrunk to three employees including Mr. Daugherty from a peak of about 40 in recent years, he said in an interview. It does not plan to file for bankruptcy, he said.

A drop in reimbursements and marketplace changes from the Affordable Care Act also played a role in LabMD's recent cuts, he said.

The FTC filed a complaint against LabMD in August alleging that the firm failed to reasonably protect data after an investigation that began in 2010. It alleged that information

on more than 9,000 consumers was found on a file-sharing network and that LabMD documents with “sensitive personal information” of at least 500 consumers was “found in the hands of identity thieves.”

The agency faulted the company for allegedly lax data-security practices and proposed an order that would require the firm to implement information-security improvements and send data-breach notices to customers.

But LabMD fought back, disputing the FTC’s authority and saying its data-security practices are covered by other laws, including the Health Insurance Portability and Accountability Act of 1996 or HIPAA, with which the firm said it was in compliance.

“The goal in this case has always been to ensure that this sensitive information is appropriately protected. FTC attorneys litigating this matter will gather information about the reported changes to LabMD’s business operations and determine how best to protect the sensitive consumer data the company has collected,” said Jessica L. Rich, director of the FTC’s bureau of consumer protection, in a statement to Risk & Compliance Journal. The bureau is litigating part of the case with LabMD.

The dispute is now playing out [in an administrative law court](#). Nonprofit group Cause of Action in November also filed a lawsuit in Washington, D.C., federal court against the FTC on behalf of LabMD.

Mr. Daugherty and Cause of Action have alleged that the FTC investigation of the alleged data security problems has been onerous. “Complying with the FTC’s demands has cost LabMD hundreds of thousands of dollars as well as thousands of hours of management and employee time,” Cause of Action said in a press release.

The FTC has tried to fill the gap left by a congressional stalemate on cybersecurity legislation, which has left the U.S. without a clear national data-security regulator. But it can be difficult for firms to know what exactly they need to do to comply with to stay on the FTC’s good side. “The agency has not issued detailed regulations to help businesses understand what sort of cybersecurity requirements it expects,” said Craig Newman, managing partner at Richards Kibbe & Orbe LLP and chief executive of the Freedom2Connect Foundation, a nonprofit organization that opposes Internet censorship.

Wyndham Worldwide Corp. has also challenged the FTC’s authority to regulate cybersecurity. The hotelier is in an ongoing legal battle with the regulator, which has faulted it for a data breach.

COMPETITION LAW 360

LabMD Winding Down Operations, Blaming FTC Suit
By Allison Grande
Jan 28 2014

Citing the “debilitating effects” of its closely watched challenge to the [Federal Trade Commission](#)'s authority to regulate private companies' data security practices, medical testing laboratory LabMD Inc. said Tuesday that it has decided to wind down its operations.

LabMD president and CEO Michael J. Daugherty said in a statement that operations at the Atlanta-based medical facility have basically ground to a halt and that although the company would “continue to meet the needs of its current clients,” it has elected to stop accepting new specimens for analysis.

The company attributed the move to its lengthy battle with the FTC, which after four years of investigation [brought an administrative action](#) in August alleging that LabMD had failed to implement reasonable and appropriate measures to prevent unauthorized access to consumers' personal data stored on its computer systems.

“LabMD's wind down is largely due to the FTC's abuse of power,” the company said Tuesday. “Absent any established or uniform data security standards; absent Congressional approval to regulate data security practices; absent a consumer victim from any alleged LabMD security breach; all without alleging that LabMD violated HIPAA privacy regulations, the FTC has spent untold taxpayer dollars investigating LabMD, destroying jobs and usurping power over patient information from the U.S. [Department of Health and Human Services](#).”

The assertions echo those LabMD has made during the course of its aggressive defense to the FTC's accusations, an effort that marks only the second time, behind a similar challenge [currently being mounted](#) by [Wyndham Worldwide Corp.](#), that a company has chosen to push back at the commission's authority to regulate the security of consumer information as an “unfair” practice under Section 5 of the FTC Act.

In both its response to the administrative complaint as well as in separate requests filed with the District of Columbia and the Eleventh Circuit to shut down the administrative proceedings, LabMD [has argued that](#) Section 5 of the FTC Act doesn't give the commission authority to regulate how a business protects consumer information, and that even if it did, the Health Insurance Portability and Accountability Act would trump it, because the information at stake is sensitive medical information.

FTC [has countered that](#) neither HIPAA nor the Health Information Technology for Economic and Clinical Health Act provides HHS with the exclusive authority over the security of consumers' sensitive personal information. Rather, the statutory framework provides the FTC and HHS with “concurrent and complementary jurisdiction” to protect consumers' sensitive health information, the agency contends.

Following the [voluntary recusal](#) of Commissioner Julie Brill, the remaining three commissioners [dealt a blow](#) to LabMD on Jan. 16, when they refused to dismiss the administrative complaint in a ruling that reiterated the commission's position that the FTC Act allowed it to regulate data security practices and bring enforcement actions targeting them.

The FTC did not immediately respond to a request for comment on LabMD's announcement Tuesday, and Daugherty was not available to provide further details on the wind down.

However, the company did attach a letter as an exhibit to a Jan. 16 filing with the Eleventh Circuit that shed more light on the matter.

In the letter to physicians, administrators, nurses and support staff, which was dated Jan. 6, Daugherty wrote that Jan. 11 would be the last day that LabMD would accept new specimens, and that the company would be closed for phone calls and Internet access after Jan. 15.

However, he added that “even during this closure, patient care is still priority number one with LabMD,” and that all reports and second opinion requests would be available for the remainder of 2014 through fax and that billing operations would also continue through the end of the year.

The letter also reiterated the company's view on the importance of its fight with the FTC, saying that the action is “a very big deal that may result in another regulator, without expertise or clear standards, standing over your shoulder with the power to destroy your practice or your company.”

Craig Newman, a managing partner of [Richards Kibbe & Orbe LLP](#) who is not connected with the case, told Law360 on Tuesday that companies should keep a careful eye on how the dispute continues to unfold, noting that it provides a “cautionary tale” to companies deciding whether they want to invest the time and money to challenge regulatory determinations.

“For the time being, the FTC has taken the position that it is regulating data protection, and there's not a court that has said anything to the contrary,” he said. “So unless businesses want to line up with Wyndham and LabMD, they will have to deal with the uncertainty of the FTC's regulations until the cases are resolved, which will likely take years.”

LabMD is represented by Reed Rubinstein and William Sherman II of [Dinsmore & Shohl LLP](#) and Michael D. Pepson of Cause of Action.

The case is In the Matter of LabMD Inc., docket number 9357, before the Federal Trade Commission.

Note: *The Office of Public Affairs compiles the FTC's Daily Clips. An archive of previous versions of [Daily Clips](#) is available in PDF format on the intranet.*

Daily Clips are an internal FTC document. You must subscribe to Clips from an @FTC.gov email address, and you may not distribute them outside the FTC.

You can unsubscribe or manage your preferences at any time by clicking the links at the bottom of this email.

If you have questions or concerns about your subscription or Daily Clips, you can contact OPA at opa@ftc.gov or call 202-326-2180.



SUBSCRIBER SERVICES: [Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This is a free service provided by the [Federal Trade Commission](#).

This email was sent to cwhite@ftc.gov using GovDelivery, on behalf of: Federal Trade Commission · 600 Pennsylvania Ave., NW · Washington, DC 20580 · 1-877-382-4357

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

DOCKET NO. 9357

**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

Kelly, Andrea

From: White, Christian S.
Sent: Friday, October 31, 2014 9:26 AM
To: VanDruff, Laura Riposo
Subject: Accepted: Teleconference

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!

In the Matter of LabMD, Inc.
Docket No. 9357
Statement of Commissioner Julie Brill
December 24, 2013

On August 28, 2013, the Commission voted unanimously to issue an administrative complaint against LabMD, Inc. (“LabMD”). The complaint alleges that LabMD exposed consumers’ sensitive personal information to unauthorized disclosure through its failure to provide reasonable and appropriate security for that information. As a result, the complaint alleges, LabMD engaged in an “unfair act or practice,” in violation of FTC Act § 5(a), 15 U.S.C. § 45(a). *See Complaint*, at 2-5 (¶¶ 6-23). LabMD denies that it violated the FTC Act. *See LabMD’s Answer and Defenses to Administrative Complaint*, at 5 (¶¶ 22-23) (Sept. 17, 2013).

On November 12 and November 26, 2013, LabMD filed two separate motions to stay the Commission’s administrative proceeding while LabMD seeks review in two federal courts of the propriety of the Commission’s administrative action against LabMD. *See generally Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings* (Nov. 12, 2013); *Motion to Stay Proceedings Pending Review in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the District of Columbia* (Nov. 26, 2013). LabMD brought the first of these federal court actions through a Verified Complaint for Declaratory Relief against the Commission filed in the U.S. District Court for the District of Columbia on November 14, 2013. On November 18, 2013, LabMD filed a “Petition for Review of Unlawful Federal Trade Commission Attempt to Regulate Patient-Information” in the U.S. Court of Appeals for the Eleventh Circuit. On December 13, 2013, the Commission unanimously denied LabMD’s motions to stay the Commission’s administrative proceeding. *See Order Denying Respondent LabMD’s Motions for Stay*, at 1 (Dec. 13, 2013).

On December 17, 2013, four days after the Commission denied LabMD’s motions to stay the administrative proceeding, LabMD filed a motion to disqualify me from further participation in this matter (“Motion to Disqualify”) on the basis of two speeches I recently delivered about data security and privacy protection in the United States, and the relationship between the U.S. and the European Union with regard to commercial privacy. On December 24, 2013, Complaint Counsel filed an opposition to the Motion to Disqualify. My statement today addresses the Motion to Disqualify. *See* 16 C.F.R. § 4.17(b)(3)(ii).

LabMD’s Motion to Disqualify is without merit. In my speeches, I provided an overview of the Commission’s enforcement work in the areas of privacy and data security. The Motion to Disqualify focuses on one or two sentences in each of these two speeches. These sentences refer in the most general of terms to the Commission’s wide range of enforcement activities. In this context, both speeches note that the Commission has “sued companies” on the basis of their data security practices. The main text does not name a specific company, nor does it discuss the specific facts in any complaint that the Commission has filed.

The only specific reference to LabMD in the two speeches is in the footnotes, which were provided to point readers to supporting documents and resources. Specifically, each speech contains a single footnote that cites the administrative complaint against LabMD as an example

of the Commission's enforcement activity in the data security area. Similarly, the neighboring citations provide examples of other enforcement actions in areas ranging from spam to children's privacy. The clear purpose of the single citation to the administrative complaint against LabMD – as well as the other citations – is to refer readers to enforcement actions that the Commission has brought in its efforts to protect consumers from a variety of privacy and data security harms.

A disinterested reader could not reasonably conclude from these two speeches that I had prejudged either the facts or the legal issues in the LabMD proceeding. *See Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1165 (D.C. Cir. 1995). The speeches cited in the Motion to Disqualify contain no explicit or implicit discussion of any facts at issue in this case, and thus bear no resemblance to the 1968 speech (of the FTC's then-Chairman Dixon) underlying the main judicial precedent on which LabMD relies. *See Cinderella Career & Finishing Schools v. FTC*, 425 F.2d 583, 589-90 (D.C. Cir. 1970). Nor do my speeches contain any discussion of how the legal standard that the Commission applies in data security cases might apply to LabMD. Simply put, the speeches contain no evidence that I had made up my mind about specific factual or legal issues in this case. *See Metropolitan Council*, 46 F.3d at 1164-65 (denying challenge to commissioners' decisions not to recuse themselves).

My speeches are designed to inform the public of the many enforcement activities that the Commission undertakes to protect consumers' privacy and security interests. *See American Medical Ass'n v. FTC*, 638 F.2d 443, 448-49 (2d Cir. 1980). In every matter that comes before the Commission, I review all of the relevant facts and arguments on all sides of the issues before reaching any conclusions. My participation in LabMD is no different. LabMD's references to the footnote citations amount to nothing more than a "vague and flimsy" suggestion to the contrary. *Metropolitan Council*, 46 F.3d at 1165.

Nevertheless, I am concerned that full adjudication of the Motion to Disqualify under Rule 4.17 would likely create an undue distraction from the important issues raised in the Commission's administrative complaint against LabMD. Allowing such a distraction to further complicate or delay adjudication of this matter would not serve the public interest. Accordingly, I recuse myself from further participation in this matter.

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

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

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

**RESPONDENT’S MOTION TO DISQUALIFY COMMISSIONER BRILL
FROM THIS ADMINISTRATIVE PROCEEDING**

Pursuant to Commission Rule 4.17, 16 C.F.R. § 4.17, Respondent LabMD, Inc. (LabMD) respectfully moves for the disqualification of Commissioner Julie Brill from this matter because her public statements show she has prejudged the facts of LabMD’s case.

In a September 17, 2013, keynote address to Forum Europe in Brussels, Belgium, Commissioner Brill said FTC has “brought myriad cases against companies that are not household names, but whose practices crossed the line.” She called out LabMD by name as the leading example of companies FTC challenged for “fail[ing] to properly secure consumer information.” Forum Europe Fourth Annual EU Data Protection and Privacy Conference, Commissioner Julie Brill’s Keynote Address, at 3 & n.15 (Sept. 17, 2013) (citing *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013) (administrative complaint) (Ex. A).

On October 29, 2013, Commissioner Brill used even more damning language, stating: “We ... have brought myriad cases against companies ... *whose practices [have] violated the law.* We’ve sued companies that ... failed to secure consumers’ personal information.” Commissioner Julie Brill’s Opening Panel Remarks, European Institute, “Data Protection,

Privacy and Security: Re-Establishing Trust Between Europe and the United States,” at 3 & n.15 (Oct. 29, 2013) (emphasis added) (Ex. B). Commissioner Brill then, once again for emphasis, cited LabMD as the leading and only culprit. *Id.* (citing *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013) (administrative complaint)).

With the exception of the LabMD matter, each Commission matter that Commissioner Brill cited as examples of Section 5 violations in the foregoing speeches is a final decision of some kind:¹ “decision and order”; “consent decree and order”; “stipulated final order”; “agreement containing consent order”; “stipulated final order”; an Article III court’s order. *See* Ex. A at 3-4 & nn. 11-23; Ex. B. at 3 nn. 9-19. *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), is a pending case before the Commission (including Commissioner Brill); LabMD has denied violating Section 5 and has exercised its right to a hearing before an ALJ; the ALJ has not made any factual findings as to LabMD’s Section 5 liability; and LabMD has filed a Motion to Dismiss with Prejudice that is currently pending before the Commission (which Commissioner Brill, along with the other Commissioners, will rule on absent disqualification).

The test for disqualification is whether “a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it.”² *Cinderella Career & Finishing Schools, Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970); *see also Nuclear Info. & Res. Serv. v. NRC*, 509 F.3d 562, 571 (D.C. Cir. 2007) (agency official should be disqualified when the “disinterested observer” standard has been met under *Cinderella*, i.e., the official “has in some measure adjudged the facts as well as the law of a

¹ Undersigned counsel learned of Commissioner Brill’s statements on Sunday, December 15, 2013.

² “[O]ur system of law has always endeavored to prevent even the probability of unfairness.” *In re Murchison*, 349 U.S. 133, 136-37 (1955). “[T]he Due Process Clause has been implemented by objective standards that do not require proof of actual bias.” *Caperton v. A. T. Massey Coal Co.*, 556 U.S. 868, 883-84 (2009).

particular case in advance of hearing it”); *Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1164-65 (D.C. Cir. 1995) (citing *Cinderella* as the standard). Here, that test has been more than met. Commissioner Brill has told the world that LabMD failed to secure consumer information and violated the law. Both of these conclusions, however, should properly follow an evidentiary hearing, not precede it.³ No neutral judge with any regard for the due process requirement of avoiding the appearance of bias and prejudgment would ever say such things about a pending case.⁴

Cinderella therefore controls and mandates Commissioner Brill’s disqualification. There, as here, a FTC commissioner made statements suggesting he had prejudged a pending case. *See Cinderella*, 425 F.2d at 589-91. In *Cinderella*, the respondent’s business “operate[d] and grant[ed] franchises for the operation of schools offering various courses in modeling, fashion merchandising, charm, and self-improvement.” *FTC v. Cinderella Career & Finishing*

³ Cf. Michael D. Pepson & John N. Sharifi, *Lego v. Twombly: The Improbable Relationship Between An Obscure Supreme Court Decision and Wrongful Convictions*, 47 AM. CRIM. L. REV. 1185, 1231-35 (2010) (arguing that institutional bias against defendants leads to erroneous factfinding and, in turn, wrongful convictions); Michael D. Pepson, Comment, *Therapeutic Jurisprudence in Philosophical Perspective*, 2 J. OF LAW, PHIL. & CULTURE 239, 260-64 (2008) (noting that the Supreme Court has said that due process requires a hearing that is more than a sham or a pretense).

⁴ Commissioner Brill’s conclusory statements that LabMD has, *in fact*, violated Section 5 are markedly different from a factual press release stating that the Commission has issued a complaint after finding “*reason to believe*” that a Section 5 violation *may* have occurred. Commissioner Brill said these things about *a hotly contested high-profile case pending before her* without using words like “allegedly” and without mentioning that she was responsible for not only ruling on LabMD’s dispositive motions in the first instance but also deciding the matter *after* a full-blown administrative adjudication. “It is fundamental that both unfairness and the appearance of unfairness should be avoided. Wherever there may be reasonable suspicion of unfairness, it is best to disqualify.” *Am. Cyanamid Co. v. FTC*, 363 F.2d 757, 767 (6th Cir. 1966). *See generally Marshall v. Jerrico, Inc.*, 446 U.S. 238, 242 (1980) (The Due Process Clause’s “neutrality requirement[, *inter alia*,] preserves both the appearance and reality of fairness, generating the feeling, so important to a popular government, that justice has been done, by ensuring that no person will be deprived of his interests in the absence of a proceeding in which he may present his case with assurance that the arbiter is not predisposed to find against him.” (citation omitted)).

Schools, Inc., 404 F.2d 1308, 1309 (D.C. Cir. 1968). FTC Chairman Dixon discussed the respondent's business model and allegedly unfair or deceptive practices in a thinly-veiled speech to a trade association and said:

What kind of vigor can a reputable newspaper exhibit? ... What standards are maintained on advertising acceptance? What would be the attitude toward accepting good money for advertising by a merchant who conducts a "going out of business" sale every five months? *What about carrying ads that offer college educations in five weeks, fortunes by raising mushrooms in the basement, getting rid of pimples with a magic lotion, or becoming an airline's hostess by attending a charm school?* Or, to raise the target a bit, how many newspapers would hesitate to accept an ad promising an unqualified guarantee for a product when the guarantee is subject to many limitations? *Granted that newspapers are not in the advertising policing business, their advertising managers are savvy enough to smell deception when the odor is strong enough.*

Cinderella, 425 F.2d at 589-90 (emphasis in original).

The *Cinderella* court disqualified Dixon for this, saying:

It requires no superior olfactory powers to recognize that the danger of unfairness through prejudgment is not diminished by a cloak of self-righteousness. We have no concern for or interest in the public statements of government officers, but we are charged with the responsibility of making certain that the image of the administrative process is not transformed from a Rubens to a Modigliani.

[T]here is in fact and law authority in the Commission, acting in the public interest, to alert the public to suspected violations of the law by factual press releases whenever the Commission shall have reason to believe that a respondent is engaged in activities made unlawful by the Act. *This does not give individual Commissioners license to prejudge cases or to make speeches which give the appearance that the case has been prejudged.* Conduct such as this may have the effect of entrenching a Commissioner in a position which he has publicly stated, making it difficult, if not impossible, for him to reach a different conclusion in the event he deems it necessary to do so after consideration of the record. There is a marked difference between the issuance of a press release which states that the Commission has filed a complaint because it has "reason to believe" that there have been violations, and statements by a Commissioner after an appeal has been filed *which give the appearance that he has already prejudged the case and that the ultimate determination of the merits will move in predestined grooves.* While these two situations—Commission press releases and a Commissioner's pre-decision public statements—are similar in appearance, they are obviously of a different order of merit.

Id. at 590 (emphasis added).

Commissioner Brill's statements are even more explicit and egregious than Dixon's. Commissioner Brill effectively stated that, in her view, LabMD's data-security practices, as a factual matter, violate Section 5. The above-cited statements were made shortly after Commissioner Brill voted to issue a Complaint against LabMD, and subsequent to LabMD's Answer denying any violation of Section 5. Commissioner Brill has thereby disposed of the fiction of FTC fairness and left no doubt about her position as to LabMD's eventual fate regardless of the outcome of its evidentiary hearing. Even before her statements, the evidence of futility was there for anyone who cared to peek inside FTC's procedural curtain and see. But Commissioner Brill has torn down this curtain and left FTC bare.

To begin with, FTC's administrative process appears to be rigged against respondents. The empirical data is that for nearly the past twenty years, in 100% of the cases where the ALJ ruled for FTC, the Commission affirmed, but in 100% of the cases where the ALJ ruled for respondent, the Commission reversed. In other words, FTC never loses.⁵

According to Commissioner Wright, the reason that the FTC's enforcement of Section 5 is fundamentally unfair arises from a combination of FTC's administrative process advantages and the vague nature of Section 5 authority. This toxic mixture gives FTC great power because, as Commissioner Wright recently told Congress, "firms typically prefer to settle Section 5 claims rather than go through the lengthy and costly administrative litigation in which they are both shooting at a moving target and may have the chips stacked against them." Preliminary Transcript, "The FTC at 100: Where Do We Go From Here?," House of Representatives,

⁵ Wright, "Recalibrating Section 5: A Response to the CPI Symposium," CPI ANTITRUST CHRONICLE, 4 (Nov. 2013), available at <https://www.competitionpolicyinternational.com/> (accessed Dec. 15, 2013).

Subcommittee on Commerce, Manufacturing, and Trade, Committee on Energy and Commerce,
at 34 (Dec. 3, 2013), available at
[http://democrats.energycommerce.house.gov/sites/default/files/documents/Preliminary-
Transcript-CMT-FTC-at-100-2013-12-3.pdf](http://democrats.energycommerce.house.gov/sites/default/files/documents/Preliminary-Transcript-CMT-FTC-at-100-2013-12-3.pdf) (accessed Dec. 16, 2013).

Unfairness and even the appearance of unfairness should be avoided by FTC. *Cinderella*,
425 F.2d at 591; *accord Am. Cyanamid Co.*, 363 F.2d at 767. No FTC official should ever take
the broad license to prejudge adjudications or to make speeches giving the clear appearance that
a matter has been decided before a fair evidentiary hearing, as Commissioner Brill has done here.
See Cinderella, 425 F.2d at 589-92. Because Commissioner Brill has “in some measure adjudged
the facts as well as the law” of LabMD’s case, she must be disqualified. *Id.* at 591.

CONCLUSION

For the foregoing reasons, we respectfully move that Commissioner Brill disqualify
herself immediately and abstain from any further participation in this matter, including, but not
limited to, participation in the Commission’s forthcoming decision on LabMD’s pending
Motion to Dismiss.

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
William Sherman II, Partner
D.C. Bar No. 1005932
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Counsel to Cause of Action

PUBLIC



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

Dated: December 17, 2013

[7]

COA # 000207
FTC-FOIA-2015-00109

EXHIBIT A

Forum Europe Fourth Annual EU Data Protection and Privacy Conference
Commissioner Julie Brill's Keynote Address
September 17, 2013
Brussels, Belgium

Good morning. I would like to thank Forum Europe for the invitation to participate in this important conference today. I am always delighted to have the opportunity to engage with my EU counterparts on issues that are important to all of us, and I see many of my friends in the audience today.

A lot has changed since this past April when I was last in Brussels. The revelations about the U.S. National Security Agency's programs¹ have sparked a global debate about government surveillance and its effect on individual privacy. As many of you know, I have spent a lifetime working on consumer protection and privacy issues, so it should be no surprise that this is a debate I welcome. It is a conversation that is long overdue, but I also think it is important that we have the right conversation—one that is open and honest, practical and productive. As we move forward with this conversation, my personal view is that there are some important facts that we should keep in mind as we collectively attempt to answer some very tough questions:

- First, whether we call privacy a “fundamental right” or a Constitutional right, the U.S., EU, and many other countries around the world place tremendous value on privacy. Our legislative and regulatory frameworks may differ, but the acknowledgment of the need for privacy protections and the principles underlying how we define those protections are, at their core, the same.²
- Second, national security exceptions in laws, including privacy laws, are the norm, not the exception, for countries around the globe, including EU Member States and third countries that have received European Commission adequacy determinations.³ As we revisit the proper scope of government surveillance, the

¹ See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (Jun. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

² See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

³ See, e.g., Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [hereinafter “EU Data Protection Directive”]; Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c. 5, 6-8, 11, available at <http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf> (Can.). See generally Christopher Wolf, *An Analysis of Service Provider Transparency Reports on Government Requests for Data*, HOGAN LOVELLS (Aug. 27, 2013), <http://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Paper-Analysis-of-Transparency-Reports.pdf>.

sufficiency of procedural safeguards, and how to “balance the ends with the means”,⁴ we should examine these issues with a global lens, as these challenges are not unique to a single sovereign.

- Third, the recent events provide a teachable moment that should encourage us to redouble our efforts on improving transparency and privacy protections for consumers in the commercial sphere. We have a renewed opportunity to be proactive rather than reactive, and to move the separate but equally important conversation about enhancing consumer privacy forward, not backward. It is important to acknowledge that commercial privacy and national security issues are two distinctly separate issues. Indeed, the EU has recognized this distinction, as the data protection laws do not apply to national security issues.⁵ And this is the right approach, helping to ensure the solutions we develop will be tailored to each set of problems we seek to address.

At the Federal Trade Commission, we address commercial privacy. We do not have criminal jurisdiction, or jurisdiction over national security issues. Of course, there are other U.S. officials who are charged with addressing those issues, and they are eager to do so.

The FTC has a long tradition of using its authority against unfair or deceptive practices to protect consumer privacy. We take action against companies that fail to comply with their own privacy policies or otherwise misrepresent their information management practices. And, just as importantly, we also address unfair collection and use of personal information that inflicts harm on consumers that they cannot reasonably avoid, and that does not offer offsetting benefits to consumers or competition.⁶

As specific privacy and data security issues have arisen over the past 40 years, Congress has supplemented the FTC’s broad remedial authority by charging us and other agencies with enforcing other privacy laws, including laws designed to protect financial⁷ and health information,⁸ children,⁹ and information used for credit, insurance, employment and housing decisions.¹⁰

⁴ Full Transcript: President Obama’s Press Conference with Swedish Prime Minister Fredrik Reinfeldt in Stockholm, WASH. POST, Sept. 4, 2013, available at http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c_story.html.

⁵ See EU Data Protection Directive, *supra* note 3, at 42.

⁶ 15 U.S.C. § 45(n).

⁷ Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.); Fair Credit Reporting Act of 1970 (FCRA), Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681u).

⁸ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. §§ 201 note, 300jj *et seq.*, 17901.

At the FTC, protecting consumer privacy is one of our most important missions. We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. Our most well-known cases – against Google,¹¹ Facebook,¹² and MySpace¹³ – have led to orders that, for the next 20 years, govern the data collection and use activities of these companies. And in each of these cases we have addressed the companies’ failure to comply with the U.S.-EU Safe Harbor.

We have also brought myriad cases against companies that are not household names, but whose practices crossed the line. We’ve sued companies spamming consumers and installing spyware on their computers.¹⁴ We’ve challenged companies that failed to properly secure consumer information.¹⁵ We have sued ad networks,¹⁶ analytics companies,¹⁷ data brokers,¹⁸ and software developers.¹⁹ We have vigorously

⁹ Children’s Online Privacy Protection Act of 1998 (COPPA), Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

¹⁰ 15 U.S.C. §§ 1681-1681t.

¹¹ In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

¹² In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

¹³ In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

¹⁴ *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>; *FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

¹⁵ *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

¹⁶ *See, e.g., In the Matter of Epic Marketplace, Inc. et al.*, FTC File No. 112 3182 (Mar. 13, 2013), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

¹⁷ *See, e.g., In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Apr. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf> (decision and order).

¹⁸ *See, e.g., U.S. v. Spokeo, Inc.*, No. 12-CV-05001 (C.D. Cal. June 19, 2012), *available at* <http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf> (consent decree and order); *In the Matter of Filiquarian Pub. LLC et al.*, FTC File No. 112 3195 (Apr. 30, 2013), *available at* <http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf> (decision and order).

¹⁹ *See, e.g., In the Matter of DesignerWare LLC*, FTC File No. 112 3151 (Apr. 11, 2013), *available at* <http://www.ftc.gov/os/caselist/1123151/designerware/130415designerwaredo.pdf> (decision and order).

enforced the Children’s Online Privacy Protection Act.²⁰ And with the world moving to mobile, we have targeted app developers as well as handheld device manufacturers engaged in inappropriate data collection and use practices.²¹

As part of our ongoing effort to address privacy issues in the changing technological landscape, just two weeks ago we brought our first action involving the Internet of Things.²² In that case, the company failed to secure the software for its Internet-accessible video cameras, which put hundreds of private lives on public display.²³

Together, these enforcement efforts have established what some scholars call “the common law of privacy” in the United States, in which the FTC articulates – to industry, defense counsel, consumer groups and other stakeholders – in an incremental, but no less effective way, the privacy practices that are deceptive or unfair.²⁴

In addition to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. We have held hearings and issued reports on cutting edge issues, including facial recognition technology²⁵, kids apps,²⁶ mobile privacy disclosures,²⁷ and mobile

²⁰ See, e.g., *U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), available at <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>.

²¹ See, e.g., *In the Matter of HTC, Inc.*, FTC File No. 122 3049 (June 25, 2013), available at <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

²² *In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), available at <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); see also Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, available at <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

²³ See *id.*

²⁴ Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014), available at <http://ssrn.com/abstract=2312913>. See also Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), (discussing how chief privacy officers reported that “state-of-the-art privacy practices” need to reflect both established black letter law and FTC cases and best practices, including FTC enforcement actions and FTC guidance); Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, BNA Privacy and Security Law Report, Oct. 25, 2010), available at http://www.justice.gov/il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf (FTC consent decrees have “created a ‘common law of consent decrees,’ producing a set of data protection rules for businesses to follow”).

²⁵ See Press Release, *FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies* (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

²⁶ See FED. TRADE COMM’N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

payments.²⁸ Last year the FTC issued its landmark privacy report in which the agency developed a new framework for addressing privacy in the U.S., including best practices for companies to follow based on three core principles: privacy by design, simplified choice, and greater transparency around data collection and use.²⁹ We called on companies to operationalize the report’s recommendations by developing better just-in-time notices and robust choice mechanisms, particularly for health and other sensitive information.³⁰

The FTC is also actively studying the data broker industry to learn more about the ways that companies collect, buy, and sell consumer data. We hope to issue a report later this year on how data brokers could improve their privacy practices.³¹ In last year’s privacy report, the FTC called on Congress to enact data broker legislation that would increase the transparency of the practices of data brokers.³²

But we don’t have to wait for legislation. I recently launched “Reclaim Your Name”, a comprehensive initiative to give consumers the means they need to reassert control over their personal data.³³ I call on industry to develop a user-friendly, one-stop online shop to provide consumers with some tools to find out about data broker practices and to exercise reasonable choices about them.³⁴ Acxiom, the largest data broker in the U.S., has taken the first step toward greater transparency by launching aboutthedata.com, a web portal that allows consumers to access, correct, and suppress the data that the company maintains about them.³⁵ And while there is certainly room for Acxiom to

²⁷ See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

²⁸ See FED. TRADE COMM’N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

²⁹ See FED. TRADE COMM’N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> [hereinafter “FTC Privacy Report”].

³⁰ See *id.*

³¹ See Press Release, FTC to Study Data Broker Industry’s Collection and Use of Consumer Data (Dec. 12, 2012), available at <http://www.ftc.gov/opa/2012/12/databrokers.shtm>.

³² See FTC Privacy Report, *supra* note 29, at 14.

³³ See Julie Brill, Commissioner, Fed. Trade Comm’n, Keynote Address at 23rd Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), available at <http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf>.

³⁴ See *id.* See also Julie Brill, Op-Ed., *Demanding Transparency from Data Brokers*, WASH. POST, Aug. 15, 2013, available at http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel.

³⁵ See generally Natasha Singer, Acxiom Lets Consumers See Data It Collects, N.Y. TIMES, Sept. 4, 2013, available at <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all>.

improve its portal, I encourage other industry players to join Axiom and step up to the plate to provide consumers with greater transparency about their data collection and use practices.

The FTC has also supported baseline privacy legislation.³⁶ The Obama Administration has been actively working on privacy legislation that would implement its Consumer Privacy Bill of Rights.³⁷

Through the FTC Act and other US privacy and data protection laws, the FTC's privacy report and other policy initiatives, and the Obama Administration's Consumer Privacy Bill of Rights, the US aims to achieve many of the same objectives that are outlined in the draft EU data protection regulation. For instance, on both sides of the Atlantic, we are striving to protect children's privacy; spur companies to implement privacy by design, increase transparency, and adopt accountability measures; and require companies to provide notice about data breaches. As the technological challenges facing the EU and the US have grown, so has our common ground in protecting consumers. In some instances, we differ on how to achieve these common goals. For example, we both believe that consumer consent is important, but we have different approaches as to when and how that consent should be obtained. The particular solutions we develop may differ, but the challenges we face and our desire to solve them are the same.

In a world with diverse privacy frameworks, interoperability is critical. We should work together to preserve existing mechanisms and develop new ways that allow our different privacy frameworks to co-exist while facilitating the flow of data across borders. The U.S.-EU Safe Harbor Framework, which enables the lawful transfer of personal data from the EU to the U.S., is vital to preserving interoperability.³⁸

Most importantly from my perspective, the Safe Harbor provides the FTC with an effective tool to protect the privacy of EU citizens. Our cases against Google, Facebook, and MySpace — which each protect EU consumers as well as American consumers, and together protect 1 billion consumers worldwide — have demonstrated the effectiveness of this Framework, as well as the FTC's determination to enforce it.

In recent months, the NSA revelations have led some to ask whether the Safe Harbor can adequately protect EU citizens' data in the commercial context. My unequivocal answer to this question is "yes." As I said before, the issue of the proper scope of government surveillance is a conversation that should happen — and will happen — on both sides of the Atlantic. But it is a conversation that should proceed outside out of the

³⁶ See FTC Privacy Report, *supra* note 29, at 13.

³⁷ See WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

³⁸ See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at http://export.gov/safeharbor/eu/eg_main_018475.asp.

commercial privacy context. In the commercial space, the Safe Harbor Framework facilitates the FTC's ability to protect the privacy of EU consumers. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

I understand that Safe Harbor, in part because of its notoriety, is an easy target, but I ask you to consider whether it is the right target. Neither the Safe Harbor nor the EU data protection directive was designed to address national security issues.³⁹ Data transferred to "adequate" countries, or through binding corporate rules, approved contractual clauses, or the Safe Harbor, are all subject to the same national security exceptions. The most salient difference is that, for transfers made pursuant to Safe Harbor, the FTC is the cop on the beat for commercial privacy issues. The same is not true of the other transfer mechanisms. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection. And, for that reason, I support its continuation.

While some things have changed since my last trip to Brussels in April, many things have remained the same. Our enforcement is still robust, including our enforcement of the Safe Harbor. Our policy development continues. And I believe that the common ground between the U.S. and the EU is still quite fertile.

Last April when I was here I quoted one of my heroes, John F. Kennedy, and I believe it is worth quoting him again. Fifty years ago, in 1963, he said: "[L]et us not be blind to our differences—but let us also direct attention to our common interests and to the means by which those differences can be resolved. And if we cannot end now our differences, at least we can help make the world safe for diversity."⁴⁰

These words continue to ring true – especially now, when we each have so much work to do to foster better consumer privacy protections for all of our citizens.

³⁹ See *id.* See also EU Data Protection Directive, *supra* note 3.

⁴⁰ See John F. Kennedy, Commencement Address at American University: Towards a Strategy of Peace (June 10, 1963), available at <http://www.jfklibrary.org/Asset-Viewer/BWC7I4C9QUmLG9J6I8oy8w.aspx>.

EXHIBIT B

Commissioner Julie Brill's Opening Panel Remarks
European Institute
Data Protection, Privacy and Security:
Re-Establishing Trust Between Europe and the United States
October 29, 2013

Good morning. I would like to thank Joëlle Attinger and the European Institute for inviting me to speak to you today. I am honored to be here with Jan Philipp Albrecht, Jim Halpert, and our esteemed colleagues from the European Parliament's LIBE committee. Welcome to Washington. I am very happy to say that we are once again open for business.

Your visit comes on the heels of a significant milestone in Brussels. Just last week, the LIBE committee reconciled thousands of amendments to the proposed EU data protection legislation, passed an initial draft, and authorized negotiations with the Council.¹

In the U.S., we have followed the EU's revision of its privacy framework closely. Although we often hear about the differences between the U.S. and EU privacy frameworks, I think it's important to highlight that we share many of the same goals. The draft EU data protection legislation that the LIBE committee approved last week adopts measures that echo many of the FTC's efforts here in the U.S., including calling on firms to:

- Adopt privacy by design;
- Increase transparency;
- Enhance consumer control;
- Improve data accuracy and consumers' access to their data;
- Strengthen data security;
- Provide parental control over information companies collect about children; and
- Encourage accountability.²

As the technological challenges facing the EU and the U.S. have grown, so has our common effort to protect consumers. In some cases, we differ on how to achieve these common goals.³ For example, we both believe that consent is important, but we have different approaches

¹ See Press Release, European Parliament Committee on Civil Liberties, Justice, and Home Affairs, Civil Liberties MEPs pave the way for stronger data protection in the EU (Oct. 21, 2013), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>.

² See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 amended (Oct. 21, 2013), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf (listing the European Parliament Committee on Civil Liberties, Justice, and Home Affairs's latest amendments to Articles 1-91); FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

as to when and how that consent should be obtained. The particular means we choose may differ, but the challenges we face and our focus on solving them are the same.

Despite our commonalities, recent events make the title of today's discussion – “Re-Establishing Trust Between Europe and the United States” – particularly relevant. There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the US and many of our European colleagues. Let me take a moment to address this issue.

Edward Snowden's disclosures about the NSA have sparked a global debate about government surveillance and its impact on individual privacy.⁴ There is great interest in the United States and in Europe in having the revelations about the NSA serve as a catalyst for change in the way governments engage in surveillance to enhance national security. As some of you know, I have spent a lifetime working on privacy issues, so it should be no surprise that this is a debate I personally welcome, as my own view is that it is a conversation that is overdue.

But I also think it is important that we have the right conversation — one that is open and honest, practical and productive. As we move forward with this conversation, we should keep in mind that consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues. I and my colleagues at the FTC focus on the appropriate balance between consumer privacy interests and commercial firms' use of consumer data, not on national security issues. And I believe the recent revelations should spur a separate and equally long overdue conversation about how we can further enhance consumer privacy and increase transparency in the commercial sphere.

The FTC is the premier U.S. consumer protection agency focused on commercial privacy. The FTC has a great track record of using its authority to go after unfair or deceptive practices that violate consumer privacy, and vigorously enforcing other laws designed to protect financial⁵ and health⁶ information, information about children⁷, and credit information used to make decisions about credit, insurance, employment, and housing.⁸

³ See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

⁴ See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (JUN. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

⁵ Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

⁶ Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. 300jj et seq. §§17901 et seq.

⁷ Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. We have brought enforcement actions against well-known companies, such as Google,⁹ Facebook,¹⁰ Twitter,¹¹ and Myspace.¹²

We have also brought myriad cases against companies that are not household names, but whose practices violated the law. We've sued companies that spammed consumers,¹³ installed spyware on computers,¹⁴ failed to secure consumers' personal information,¹⁵ deceptively tracked consumers online,¹⁶ violated children's privacy laws,¹⁷ inappropriately collected information on consumers' mobile devices,¹⁸ and failed to secure Internet-connected devices.¹⁹ We have obtained millions of dollars in penalties and restitution in our privacy and data security cases, and placed numerous companies under 20-year orders with robust injunctive provisions.

⁸ Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

⁹ In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

¹⁰ In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

¹¹ In the Matter of Twitter, Inc., FTC File No. 092 3093 (March 3, 2011) *available at* <http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf> (decision and order).

¹² In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

¹³ *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>.

¹⁴ *See, e.g., FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

¹⁵ *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

¹⁶ *See, e.g., In the Matter of Epic Marketplace, Inc., et al.*, FTC File No. 112 3182 (Dec. 5, 2012), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

¹⁷ *See, e.g., U.S. v. Artist Arena, LLC*, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf> (stipulated final order).

¹⁸ *See U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), *available at* <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>; In the Matter of HTC, Inc., FTC File No. 122 3049 (June 25, 2013), *available at* <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

¹⁹ *See In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), *available at* <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); *see also* Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, *available at* <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

As a complement to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. In addition to our landmark privacy report issued last year, we have addressed cutting-edge privacy issues involving facial recognition technology,²⁰ kids apps,²¹ mobile privacy disclosures,²² and mobile payments.²³

In light of our increasingly interconnected world, the FTC has devoted significant time to enhancing international privacy enforcement cooperation so that we are better able to address global challenges. We continue to foster a strong relationship and engage in ongoing dialogue with European data protection authorities. We meet regularly with EU DPAs, and in April I met with the entire Article 29 Working Party. The Article 29 Working Party has been kind enough to recognize the FTC as a crucial partner in privacy and data protection enforcement.²⁴ And the Working Party, like the FTC, has welcomed the ongoing dialogue and constructive cooperation between us, and stressed the need for further transatlantic cooperation, especially in enforcement matters, in order to achieve our common goals.²⁵ Indeed, the FTC's recent Memorandum of Understanding with the Irish DPA establishes a good framework for increased, more streamlined, and more effective privacy enforcement cooperation.²⁶ And just last month, we worked very closely with our EU and Canadian counterparts to launch the International Conference of Data Protection and Privacy Commissioners' initiative to address challenges in global privacy enforcement cooperation.²⁷

²⁰ See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

²¹ See FED. TRADE COMM'N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

²² See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

²³ See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

²⁴ Press Release, Article 29 Data Protection Working Party Meeting with FTC Commissioner Julie Brill (Apr. 29, 2013), available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130429_pr_april_plenary_en.pdf.

²⁵ See *Id.*

²⁶ Memorandum of Understanding Regarding Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, U.S. FED. TRADE COMM'N-DATA PROTECTION COMMISSIONER OF IRELAND, June 2013, available at <http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf>.

²⁷ See Resolution on International Enforcement and Cooperation, 35th International Conference of Data Protection and Privacy Commissioners, Sept. 23-26, 2013, available at <https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf>.

Another critical role played by the FTC is to enforce the U.S.-EU Safe Harbor framework.²⁸ We know that Safe Harbor has received its share of criticism, particularly in the past few months. We've read the news reports and heard about the recent Parliamentary hearings about Safe Harbor.²⁹ Given the active debate over Safe Harbor right now, I'd like to address head-on the contention in some quarters that Safe Harbor isn't up to the job of protecting EU citizens' data in the commercial sphere.

First, the FTC vigorously enforces the Safe Harbor. As the Safe Harbor program has grown over the past decade, so has the FTC's enforcement activity. Since 2009, we have brought ten Safe Harbor cases.³⁰ When Safe Harbor was established, the FTC committed to review on a priority basis all referrals from EU member state authorities.³¹ With few referrals over the past decade, we have taken the initiative to proactively look for Safe Harbor violations in every privacy and data security investigation we conduct. That is how we discovered the Safe Harbor violations of Google, Facebook, and Myspace in the last few years. These cases demonstrate the enforceability of Safe Harbor certifications and the high cost that companies can pay for non-compliance. The orders in Google, Facebook, and Myspace require the companies to implement comprehensive privacy programs and subject the companies to ongoing privacy audits for 20 years.³² Violations of these orders can result in hefty fines, as Google discovered when we assessed a \$22.5 million civil penalty against the company last year for violating its consent decree.³³ The FTC orders against Google, Facebook, and Myspace help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe. These cases demonstrate that Safe Harbor gives the FTC an effective and functioning tool to protect the privacy of EU citizen data transferred to America. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

Second, going forward, the FTC will continue to make the Safe Harbor a top enforcement priority. Indeed, we have opened numerous investigations into Safe Harbor compliance in recent months. We will continue to welcome any substantive leads, such as the complaint we received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations. And, let me be clear, we take this recent complaint very seriously. Of

²⁸ See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at http://export.gov/safeharbor/eu/eg_main_018475.asp.

²⁹ See LIBE Committee *Inquiry on Electronic Mass Surveillance of EU Citizens, Sixth Hearing* (Oct. 7, 2013), available at <http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE>.

³⁰ See Legal Resources, Bureau of Consumer Protection Business Center, U.S. FED. TRADE COMM'N, available at <http://business.ftc.gov/legal-resources/2840/3>.

³¹ See Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n to John Mogg, Director, Directorate-General XV, European Commission (Jul. 14, 2000), available at http://export.gov/static/sh_en FTCLETTERFINAL Latest eg_main_018455.pdf.

³² See Google, *supra* note 9; Facebook, *supra* note 10; Myspace, *supra* note 12.

³³ See Press Release, Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), available at <http://ftc.gov/opa/2012/08/google.shtm>.

course, as we do in every instance, we take the necessary time to separate fact from fiction. And, as I am sure many in this audience would appreciate, we also proceed carefully to provide proper notice and appropriate levels of due process. If we discover in our investigations that companies have committed Safe Harbor-related law violations, we will take appropriate enforcement actions.

As I mentioned earlier, I think it is healthy to have a vigorous debate over how to appropriately balance national security and privacy, but that ongoing debate should not be allowed to distort discussions in the commercial sphere about role of the Safe Harbor in protection consumer privacy. The EU itself has created national security exemptions in its existing data protection laws,³⁴ and the European Commission proposed such exemptions for government surveillance in its draft data protection regulation.³⁵ In other words, the EU has justifiably recognized the need to tackle their member states' national security issues separately. Safe Harbor is no different and warrants a similar approach. Just as the EU Data Protection Directive was not designed to address national security issues, neither was the Safe Harbor. Whatever the means to transfer data about European consumers for commercial purposes – whether to countries whose laws are deemed “adequate”, through approved contractual clauses, or by way of the Safe Harbor – all these transfer mechanisms are subject to national security exceptions. The difference is that, for Safe Harbor violations, the FTC is the cop on the beat. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection.

I know that some of you in this room may have taken a different view of the Safe Harbor framework. I hope my thoughts give you cause to reexamine the virtues of the Safe Harbor system. As the draft regulation continues its journey through the process of review and adoption, I am hopeful that we can continue to work together to promote both the free flow of data and strong consumer privacy protections.

And while it may not make the headlines or the nightly news, in the midst of all of the recent developments at home and across the pond, our efforts to enhance privacy enforcement cooperation continue to build trust day by day. We want to continue to develop these ties of cross border law enforcement cooperation – including Safe Harbor enforcement – that enhance privacy and data security – as these are the ties that build rather than erode trust, the ties that bind rather than divide us. We have worked extensively with our friends in the EU on these and other issues, and we look forward to continuing that collaboration to enhance privacy protection for consumers on both sides of the Atlantic.

Thank you.

³⁴ Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

³⁵ See *Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11. final (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

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

**[PROPOSED] ORDER GRANTING RESPONDENT’S MOTION TO DISQUALIFY
COMMISSIONER BRILL FROM THIS ADMINISTRATIVE PROCEEDING**

This matter came before the Commission on December 17, 2013, upon a Motion to Disqualify Commissioner Brill From This Administrative Proceeding (Motion) filed by Respondent LabMD, Inc. (LabMD) pursuant to Commission Rule 4.17, 16 C.F.R. § 4.17, for an Order disqualifying Commissioner Julie Brill from participation in the above-captioned matter. Having considered LabMD’s Motion and all supporting papers, and good cause appearing,

IT IS ORDERED THAT LabMD’s Motion **IS GRANTED;** and

IT IS FURTHER ORDERED THAT Commissioner Brill is disqualified from participating in the above-captioned matter, including but not limited to any vote concerning the above-captioned matter and the Commission’s forthcoming decision on LabMD’s pending Motion to Dismiss the Complaint with Prejudice.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED:

CERTIFICATE OF SERVICE

I hereby certify that on December 17, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

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

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

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


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

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

CERTIFICATE OF ELECTRONIC FILING

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

Dated: December 17, 2013

By 
Michael D. Pepson

(b)(5)

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.

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

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

**RESPONDENT’S MOTION TO DISQUALIFY COMMISSIONER BRILL
FROM THIS ADMINISTRATIVE PROCEEDING**

Pursuant to Commission Rule 4.17, 16 C.F.R. § 4.17, Respondent LabMD, Inc. (LabMD) respectfully moves for the disqualification of Commissioner Julie Brill from this matter because her public statements show she has prejudged the facts of LabMD’s case.

In a September 17, 2013, keynote address to Forum Europe in Brussels, Belgium, Commissioner Brill said FTC has “brought myriad cases against companies that are not household names, but whose practices crossed the line.” She called out LabMD by name as the leading example of companies FTC challenged for “fail[ing] to properly secure consumer information.” Forum Europe Fourth Annual EU Data Protection and Privacy Conference, Commissioner Julie Brill’s Keynote Address, at 3 & n.15 (Sept. 17, 2013) (citing *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013) (administrative complaint) (Ex. A).

On October 29, 2013, Commissioner Brill used even more damning language, stating: “We ... have brought myriad cases against companies ... *whose practices [have] violated the law.* We’ve sued companies that ... failed to secure consumers’ personal information.” Commissioner Julie Brill’s Opening Panel Remarks, European Institute, “Data Protection,

Privacy and Security: Re-Establishing Trust Between Europe and the United States,” at 3 & n.15 (Oct. 29, 2013) (emphasis added) (Ex. B). Commissioner Brill then, once again for emphasis, cited LabMD as the leading and only culprit. *Id.* (citing *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013) (administrative complaint)).

With the exception of the LabMD matter, each Commission matter that Commissioner Brill cited as examples of Section 5 violations in the foregoing speeches is a final decision of some kind:¹ “decision and order”; “consent decree and order”; “stipulated final order”; “agreement containing consent order”; “stipulated final order”; an Article III court’s order. *See* Ex. A at 3-4 & nn. 11-23; Ex. B. at 3 nn. 9-19. *In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), is a pending case before the Commission (including Commissioner Brill); LabMD has denied violating Section 5 and has exercised its right to a hearing before an ALJ; the ALJ has not made any factual findings as to LabMD’s Section 5 liability; and LabMD has filed a Motion to Dismiss with Prejudice that is currently pending before the Commission (which Commissioner Brill, along with the other Commissioners, will rule on absent disqualification).

The test for disqualification is whether “a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it.”² *Cinderella Career & Finishing Schools, Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970); *see also Nuclear Info. & Res. Serv. v. NRC*, 509 F.3d 562, 571 (D.C. Cir. 2007) (agency official should be disqualified when the “disinterested observer” standard has been met under *Cinderella*, i.e., the official “has in some measure adjudged the facts as well as the law of a

¹ Undersigned counsel learned of Commissioner Brill’s statements on Sunday, December 15, 2013.

² “[O]ur system of law has always endeavored to prevent even the probability of unfairness.” *In re Murchison*, 349 U.S. 133, 136-37 (1955). “[T]he Due Process Clause has been implemented by objective standards that do not require proof of actual bias.” *Caperton v. A. T. Massey Coal Co.*, 556 U.S. 868, 883-84 (2009).

particular case in advance of hearing it”); *Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1164-65 (D.C. Cir. 1995) (citing *Cinderella* as the standard). Here, that test has been more than met. Commissioner Brill has told the world that LabMD failed to secure consumer information and violated the law. Both of these conclusions, however, should properly follow an evidentiary hearing, not precede it.³ No neutral judge with any regard for the due process requirement of avoiding the appearance of bias and prejudgment would ever say such things about a pending case.⁴

Cinderella therefore controls and mandates Commissioner Brill’s disqualification. There, as here, a FTC commissioner made statements suggesting he had prejudged a pending case. *See Cinderella*, 425 F.2d at 589-91. In *Cinderella*, the respondent’s business “operate[d] and grant[ed] franchises for the operation of schools offering various courses in modeling, fashion merchandising, charm, and self-improvement.” *FTC v. Cinderella Career & Finishing*

³ Cf. Michael D. Pepson & John N. Sharifi, *Lego v. Twombly: The Improbable Relationship Between An Obscure Supreme Court Decision and Wrongful Convictions*, 47 AM. CRIM. L. REV. 1185, 1231-35 (2010) (arguing that institutional bias against defendants leads to erroneous factfinding and, in turn, wrongful convictions); Michael D. Pepson, Comment, *Therapeutic Jurisprudence in Philosophical Perspective*, 2 J. OF LAW, PHIL. & CULTURE 239, 260-64 (2008) (noting that the Supreme Court has said that due process requires a hearing that is more than a sham or a pretense).

⁴ Commissioner Brill’s conclusory statements that LabMD has, *in fact*, violated Section 5 are markedly different from a factual press release stating that the Commission has issued a complaint after finding “*reason to believe*” that a Section 5 violation *may* have occurred. Commissioner Brill said these things about *a hotly contested high-profile case pending before her* without using words like “allegedly” and without mentioning that she was responsible for not only ruling on LabMD’s dispositive motions in the first instance but also deciding the matter *after* a full-blown administrative adjudication. “It is fundamental that both unfairness and the appearance of unfairness should be avoided. Wherever there may be reasonable suspicion of unfairness, it is best to disqualify.” *Am. Cyanamid Co. v. FTC*, 363 F.2d 757, 767 (6th Cir. 1966). *See generally Marshall v. Jerrico, Inc.*, 446 U.S. 238, 242 (1980) (The Due Process Clause’s “neutrality requirement[, *inter alia*,] preserves both the appearance and reality of fairness, generating the feeling, so important to a popular government, that justice has been done, by ensuring that no person will be deprived of his interests in the absence of a proceeding in which he may present his case with assurance that the arbiter is not predisposed to find against him.” (citation omitted)).

Schools, Inc., 404 F.2d 1308, 1309 (D.C. Cir. 1968). FTC Chairman Dixon discussed the respondent's business model and allegedly unfair or deceptive practices in a thinly-veiled speech to a trade association and said:

What kind of vigor can a reputable newspaper exhibit? ... What standards are maintained on advertising acceptance? What would be the attitude toward accepting good money for advertising by a merchant who conducts a "going out of business" sale every five months? *What about carrying ads that offer college educations in five weeks, fortunes by raising mushrooms in the basement, getting rid of pimples with a magic lotion, or becoming an airline's hostess by attending a charm school?* Or, to raise the target a bit, how many newspapers would hesitate to accept an ad promising an unqualified guarantee for a product when the guarantee is subject to many limitations? *Granted that newspapers are not in the advertising policing business, their advertising managers are savvy enough to smell deception when the odor is strong enough.*

Cinderella, 425 F.2d at 589-90 (emphasis in original).

The *Cinderella* court disqualified Dixon for this, saying:

It requires no superior olfactory powers to recognize that the danger of unfairness through prejudgment is not diminished by a cloak of self-righteousness. We have no concern for or interest in the public statements of government officers, but we are charged with the responsibility of making certain that the image of the administrative process is not transformed from a Rubens to a Modigliani.

[T]here is in fact and law authority in the Commission, acting in the public interest, to alert the public to suspected violations of the law by factual press releases whenever the Commission shall have reason to believe that a respondent is engaged in activities made unlawful by the Act. *This does not give individual Commissioners license to prejudge cases or to make speeches which give the appearance that the case has been prejudged.* Conduct such as this may have the effect of entrenching a Commissioner in a position which he has publicly stated, making it difficult, if not impossible, for him to reach a different conclusion in the event he deems it necessary to do so after consideration of the record. There is a marked difference between the issuance of a press release which states that the Commission has filed a complaint because it has "reason to believe" that there have been violations, and statements by a Commissioner after an appeal has been filed *which give the appearance that he has already prejudged the case and that the ultimate determination of the merits will move in predestined grooves.* While these two situations—Commission press releases and a Commissioner's pre-decision public statements—are similar in appearance, they are obviously of a different order of merit.

Id. at 590 (emphasis added).

Commissioner Brill's statements are even more explicit and egregious than Dixon's. Commissioner Brill effectively stated that, in her view, LabMD's data-security practices, as a factual matter, violate Section 5. The above-cited statements were made shortly after Commissioner Brill voted to issue a Complaint against LabMD, and subsequent to LabMD's Answer denying any violation of Section 5. Commissioner Brill has thereby disposed of the fiction of FTC fairness and left no doubt about her position as to LabMD's eventual fate regardless of the outcome of its evidentiary hearing. Even before her statements, the evidence of futility was there for anyone who cared to peek inside FTC's procedural curtain and see. But Commissioner Brill has torn down this curtain and left FTC bare.

To begin with, FTC's administrative process appears to be rigged against respondents. The empirical data is that for nearly the past twenty years, in 100% of the cases where the ALJ ruled for FTC, the Commission affirmed, but in 100% of the cases where the ALJ ruled for respondent, the Commission reversed. In other words, FTC never loses.⁵

According to Commissioner Wright, the reason that the FTC's enforcement of Section 5 is fundamentally unfair arises from a combination of FTC's administrative process advantages and the vague nature of Section 5 authority. This toxic mixture gives FTC great power because, as Commissioner Wright recently told Congress, "firms typically prefer to settle Section 5 claims rather than go through the lengthy and costly administrative litigation in which they are both shooting at a moving target and may have the chips stacked against them." Preliminary Transcript, "The FTC at 100: Where Do We Go From Here?," House of Representatives,

⁵ Wright, "Recalibrating Section 5: A Response to the CPI Symposium," CPI ANTITRUST CHRONICLE, 4 (Nov. 2013), available at <https://www.competitionpolicyinternational.com/> (accessed Dec. 15, 2013).

Subcommittee on Commerce, Manufacturing, and Trade, Committee on Energy and Commerce,
at 34 (Dec. 3, 2013), available at
[http://democrats.energycommerce.house.gov/sites/default/files/documents/Preliminary-
Transcript-CMT-FTC-at-100-2013-12-3.pdf](http://democrats.energycommerce.house.gov/sites/default/files/documents/Preliminary-Transcript-CMT-FTC-at-100-2013-12-3.pdf) (accessed Dec. 16, 2013).

Unfairness and even the appearance of unfairness should be avoided by FTC. *Cinderella*,
425 F.2d at 591; *accord Am. Cyanamid Co.*, 363 F.2d at 767. No FTC official should ever take
the broad license to prejudge adjudications or to make speeches giving the clear appearance that
a matter has been decided before a fair evidentiary hearing, as Commissioner Brill has done here.
See Cinderella, 425 F.2d at 589-92. Because Commissioner Brill has “in some measure adjudged
the facts as well as the law” of LabMD’s case, she must be disqualified. *Id.* at 591.

CONCLUSION

For the foregoing reasons, we respectfully move that Commissioner Brill disqualify
herself immediately and abstain from any further participation in this matter, including, but not
limited to, participation in the Commission’s forthcoming decision on LabMD’s pending
Motion to Dismiss.

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
William Sherman II, Partner
D.C. Bar No. 1005932
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Counsel to Cause of Action

PUBLIC



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

Dated: December 17, 2013

[7]

COA # 000233
FTC-FOIA-2015-00109

EXHIBIT A

Forum Europe Fourth Annual EU Data Protection and Privacy Conference
Commissioner Julie Brill's Keynote Address
September 17, 2013
Brussels, Belgium

Good morning. I would like to thank Forum Europe for the invitation to participate in this important conference today. I am always delighted to have the opportunity to engage with my EU counterparts on issues that are important to all of us, and I see many of my friends in the audience today.

A lot has changed since this past April when I was last in Brussels. The revelations about the U.S. National Security Agency's programs¹ have sparked a global debate about government surveillance and its effect on individual privacy. As many of you know, I have spent a lifetime working on consumer protection and privacy issues, so it should be no surprise that this is a debate I welcome. It is a conversation that is long overdue, but I also think it is important that we have the right conversation—one that is open and honest, practical and productive. As we move forward with this conversation, my personal view is that there are some important facts that we should keep in mind as we collectively attempt to answer some very tough questions:

- First, whether we call privacy a “fundamental right” or a Constitutional right, the U.S., EU, and many other countries around the world place tremendous value on privacy. Our legislative and regulatory frameworks may differ, but the acknowledgment of the need for privacy protections and the principles underlying how we define those protections are, at their core, the same.²
- Second, national security exceptions in laws, including privacy laws, are the norm, not the exception, for countries around the globe, including EU Member States and third countries that have received European Commission adequacy determinations.³ As we revisit the proper scope of government surveillance, the

¹ See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (Jun. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

² See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

³ See, e.g., Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [hereinafter “EU Data Protection Directive”]; Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c. 5, 6-8, 11, available at <http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf> (Can.). See generally Christopher Wolf, *An Analysis of Service Provider Transparency Reports on Government Requests for Data*, HOGAN LOVELLS (Aug. 27, 2013), <http://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Paper-Analysis-of-Transparency-Reports.pdf>.

sufficiency of procedural safeguards, and how to “balance the ends with the means”,⁴ we should examine these issues with a global lens, as these challenges are not unique to a single sovereign.

- Third, the recent events provide a teachable moment that should encourage us to redouble our efforts on improving transparency and privacy protections for consumers in the commercial sphere. We have a renewed opportunity to be proactive rather than reactive, and to move the separate but equally important conversation about enhancing consumer privacy forward, not backward. It is important to acknowledge that commercial privacy and national security issues are two distinctly separate issues. Indeed, the EU has recognized this distinction, as the data protection laws do not apply to national security issues.⁵ And this is the right approach, helping to ensure the solutions we develop will be tailored to each set of problems we seek to address.

At the Federal Trade Commission, we address commercial privacy. We do not have criminal jurisdiction, or jurisdiction over national security issues. Of course, there are other U.S. officials who are charged with addressing those issues, and they are eager to do so.

The FTC has a long tradition of using its authority against unfair or deceptive practices to protect consumer privacy. We take action against companies that fail to comply with their own privacy policies or otherwise misrepresent their information management practices. And, just as importantly, we also address unfair collection and use of personal information that inflicts harm on consumers that they cannot reasonably avoid, and that does not offer offsetting benefits to consumers or competition.⁶

As specific privacy and data security issues have arisen over the past 40 years, Congress has supplemented the FTC’s broad remedial authority by charging us and other agencies with enforcing other privacy laws, including laws designed to protect financial⁷ and health information,⁸ children,⁹ and information used for credit, insurance, employment and housing decisions.¹⁰

⁴ Full Transcript: President Obama’s Press Conference with Swedish Prime Minister Fredrik Reinfeldt in Stockholm, WASH. POST, Sept. 4, 2013, available at http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c_story.html.

⁵ See EU Data Protection Directive, *supra* note 3, at 42.

⁶ 15 U.S.C. § 45(n).

⁷ Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.); Fair Credit Reporting Act of 1970 (FCRA), Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681u).

⁸ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. §§ 201 note, 300jj *et seq.*, 17901....

At the FTC, protecting consumer privacy is one of our most important missions. We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. Our most well-known cases – against Google,¹¹ Facebook,¹² and MySpace¹³ – have led to orders that, for the next 20 years, govern the data collection and use activities of these companies. And in each of these cases we have addressed the companies’ failure to comply with the U.S.-EU Safe Harbor.

We have also brought myriad cases against companies that are not household names, but whose practices crossed the line. We’ve sued companies spamming consumers and installing spyware on their computers.¹⁴ We’ve challenged companies that failed to properly secure consumer information.¹⁵ We have sued ad networks,¹⁶ analytics companies,¹⁷ data brokers,¹⁸ and software developers.¹⁹ We have vigorously

⁹ Children’s Online Privacy Protection Act of 1998 (COPPA), Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

¹⁰ 15 U.S.C. §§ 1681-1681t.

¹¹ In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

¹² In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

¹³ In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

¹⁴ *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>; *FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

¹⁵ *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

¹⁶ *See, e.g., In the Matter of Epic Marketplace, Inc. et al.*, FTC File No. 112 3182 (Mar. 13, 2013), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

¹⁷ *See, e.g., In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Apr. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf> (decision and order).

¹⁸ *See, e.g., U.S. v. Spokeo, Inc.*, No. 12-CV-05001 (C.D. Cal. June 19, 2012), *available at* <http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf> (consent decree and order); *In the Matter of Filiquarian Pub. LLC et al.*, FTC File No. 112 3195 (Apr. 30, 2013), *available at* <http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf> (decision and order).

¹⁹ *See, e.g., In the Matter of DesignerWare LLC*, FTC File No. 112 3151 (Apr. 11, 2013), *available at* <http://www.ftc.gov/os/caselist/1123151/designerware/130415designerwaredo.pdf> (decision and order).

enforced the Children’s Online Privacy Protection Act.²⁰ And with the world moving to mobile, we have targeted app developers as well as handheld device manufacturers engaged in inappropriate data collection and use practices.²¹

As part of our ongoing effort to address privacy issues in the changing technological landscape, just two weeks ago we brought our first action involving the Internet of Things.²² In that case, the company failed to secure the software for its Internet-accessible video cameras, which put hundreds of private lives on public display.²³

Together, these enforcement efforts have established what some scholars call “the common law of privacy” in the United States, in which the FTC articulates – to industry, defense counsel, consumer groups and other stakeholders – in an incremental, but no less effective way, the privacy practices that are deceptive or unfair.²⁴

In addition to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. We have held hearings and issued reports on cutting edge issues, including facial recognition technology²⁵, kids apps,²⁶ mobile privacy disclosures,²⁷ and mobile

²⁰ See, e.g., *U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), available at <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>.

²¹ See, e.g., In the Matter of HTC, Inc., FTC File No. 122 3049 (June 25, 2013), available at <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

²² In the Matter of TRENDnet, Inc., FTC File No. 122 3090 (Sept. 4, 2013), available at <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); see also Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, available at <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

²³ See *id.*

²⁴ Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014), available at <http://ssrn.com/abstract=2312913>. See also Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), (discussing how chief privacy officers reported that “state-of-the-art privacy practices” need to reflect both established black letter law and FTC cases and best practices, including FTC enforcement actions and FTC guidance); Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States*, BNA Privacy and Security Law Report, Oct. 25, 2010), available at http://www.justice.gov/il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf (FTC consent decrees have “created a ‘common law of consent decrees,’ producing a set of data protection rules for businesses to follow”).

²⁵ See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

²⁶ See FED. TRADE COMM’N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

payments.²⁸ Last year the FTC issued its landmark privacy report in which the agency developed a new framework for addressing privacy in the U.S., including best practices for companies to follow based on three core principles: privacy by design, simplified choice, and greater transparency around data collection and use.²⁹ We called on companies to operationalize the report's recommendations by developing better just-in-time notices and robust choice mechanisms, particularly for health and other sensitive information.³⁰

The FTC is also actively studying the data broker industry to learn more about the ways that companies collect, buy, and sell consumer data. We hope to issue a report later this year on how data brokers could improve their privacy practices.³¹ In last year's privacy report, the FTC called on Congress to enact data broker legislation that would increase the transparency of the practices of data brokers.³²

But we don't have to wait for legislation. I recently launched "Reclaim Your Name", a comprehensive initiative to give consumers the means they need to reassert control over their personal data.³³ I call on industry to develop a user-friendly, one-stop online shop to provide consumers with some tools to find out about data broker practices and to exercise reasonable choices about them.³⁴ Acxiom, the largest data broker in the U.S., has taken the first step toward greater transparency by launching aboutthedata.com, a web portal that allows consumers to access, correct, and suppress the data that the company maintains about them.³⁵ And while there is certainly room for Acxiom to

²⁷ See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

²⁸ See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

²⁹ See FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> [hereinafter "FTC Privacy Report"].

³⁰ See *id.*

³¹ See Press Release, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 12, 2012), available at <http://www.ftc.gov/opa/2012/12/databrokers.shtm>.

³² See FTC Privacy Report, *supra* note 29, at 14.

³³ See Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at 23rd Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), available at <http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf>.

³⁴ See *id.* See also Julie Brill, Op-Ed., *Demanding Transparency from Data Brokers*, WASH. POST, Aug. 15, 2013, available at http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel.

³⁵ See generally Natasha Singer, Acxiom Lets Consumers See Data It Collects, N.Y. TIMES, Sept. 4, 2013, available at <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all>.

improve its portal, I encourage other industry players to join Axiom and step up to the plate to provide consumers with greater transparency about their data collection and use practices.

The FTC has also supported baseline privacy legislation.³⁶ The Obama Administration has been actively working on privacy legislation that would implement its Consumer Privacy Bill of Rights.³⁷

Through the FTC Act and other US privacy and data protection laws, the FTC's privacy report and other policy initiatives, and the Obama Administration's Consumer Privacy Bill of Rights, the US aims to achieve many of the same objectives that are outlined in the draft EU data protection regulation. For instance, on both sides of the Atlantic, we are striving to protect children's privacy; spur companies to implement privacy by design, increase transparency, and adopt accountability measures; and require companies to provide notice about data breaches. As the technological challenges facing the EU and the US have grown, so has our common ground in protecting consumers. In some instances, we differ on how to achieve these common goals. For example, we both believe that consumer consent is important, but we have different approaches as to when and how that consent should be obtained. The particular solutions we develop may differ, but the challenges we face and our desire to solve them are the same.

In a world with diverse privacy frameworks, interoperability is critical. We should work together to preserve existing mechanisms and develop new ways that allow our different privacy frameworks to co-exist while facilitating the flow of data across borders. The U.S.-EU Safe Harbor Framework, which enables the lawful transfer of personal data from the EU to the U.S., is vital to preserving interoperability.³⁸

Most importantly from my perspective, the Safe Harbor provides the FTC with an effective tool to protect the privacy of EU citizens. Our cases against Google, Facebook, and MySpace — which each protect EU consumers as well as American consumers, and together protect 1 billion consumers worldwide — have demonstrated the effectiveness of this Framework, as well as the FTC's determination to enforce it.

In recent months, the NSA revelations have led some to ask whether the Safe Harbor can adequately protect EU citizens' data in the commercial context. My unequivocal answer to this question is "yes." As I said before, the issue of the proper scope of government surveillance is a conversation that should happen — and will happen — on both sides of the Atlantic. But it is a conversation that should proceed outside out of the

³⁶ See FTC Privacy Report, *supra* note 29, at 13.

³⁷ See WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

³⁸ See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at http://export.gov/safeharbor/eu/eg_main_018475.asp.

commercial privacy context. In the commercial space, the Safe Harbor Framework facilitates the FTC's ability to protect the privacy of EU consumers. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

I understand that Safe Harbor, in part because of its notoriety, is an easy target, but I ask you to consider whether it is the right target. Neither the Safe Harbor nor the EU data protection directive was designed to address national security issues.³⁹ Data transferred to "adequate" countries, or through binding corporate rules, approved contractual clauses, or the Safe Harbor, are all subject to the same national security exceptions. The most salient difference is that, for transfers made pursuant to Safe Harbor, the FTC is the cop on the beat for commercial privacy issues. The same is not true of the other transfer mechanisms. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection. And, for that reason, I support its continuation.

While some things have changed since my last trip to Brussels in April, many things have remained the same. Our enforcement is still robust, including our enforcement of the Safe Harbor. Our policy development continues. And I believe that the common ground between the U.S. and the EU is still quite fertile.

Last April when I was here I quoted one of my heroes, John F. Kennedy, and I believe it is worth quoting him again. Fifty years ago, in 1963, he said: "[L]et us not be blind to our differences—but let us also direct attention to our common interests and to the means by which those differences can be resolved. And if we cannot end now our differences, at least we can help make the world safe for diversity."⁴⁰

These words continue to ring true – especially now, when we each have so much work to do to foster better consumer privacy protections for all of our citizens.

³⁹ See *id.* See also EU Data Protection Directive, *supra* note 3.

⁴⁰ See John F. Kennedy, Commencement Address at American University: Towards a Strategy of Peace (June 10, 1963), available at <http://www.jfklibrary.org/Asset-Viewer/BWC7I4C9QUmLG9J6I8oy8w.aspx>.

EXHIBIT B

Commissioner Julie Brill's Opening Panel Remarks
European Institute
Data Protection, Privacy and Security:
Re-Establishing Trust Between Europe and the United States
October 29, 2013

Good morning. I would like to thank Joëlle Attinger and the European Institute for inviting me to speak to you today. I am honored to be here with Jan Philipp Albrecht, Jim Halpert, and our esteemed colleagues from the European Parliament's LIBE committee. Welcome to Washington. I am very happy to say that we are once again open for business.

Your visit comes on the heels of a significant milestone in Brussels. Just last week, the LIBE committee reconciled thousands of amendments to the proposed EU data protection legislation, passed an initial draft, and authorized negotiations with the Council.¹

In the U.S., we have followed the EU's revision of its privacy framework closely. Although we often hear about the differences between the U.S. and EU privacy frameworks, I think it's important to highlight that we share many of the same goals. The draft EU data protection legislation that the LIBE committee approved last week adopts measures that echo many of the FTC's efforts here in the U.S., including calling on firms to:

- Adopt privacy by design;
- Increase transparency;
- Enhance consumer control;
- Improve data accuracy and consumers' access to their data;
- Strengthen data security;
- Provide parental control over information companies collect about children; and
- Encourage accountability.²

As the technological challenges facing the EU and the U.S. have grown, so has our common effort to protect consumers. In some cases, we differ on how to achieve these common goals.³ For example, we both believe that consent is important, but we have different approaches

¹ See Press Release, European Parliament Committee on Civil Liberties, Justice, and Home Affairs, Civil Liberties MEPs pave the way for stronger data protection in the EU (Oct. 21, 2013), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>.

² See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 amended (Oct. 21, 2013), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf (listing the European Parliament Committee on Civil Liberties, Justice, and Home Affairs's latest amendments to Articles 1-91); FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

as to when and how that consent should be obtained. The particular means we choose may differ, but the challenges we face and our focus on solving them are the same.

Despite our commonalities, recent events make the title of today's discussion – “Re-Establishing Trust Between Europe and the United States” – particularly relevant. There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the US and many of our European colleagues. Let me take a moment to address this issue.

Edward Snowden's disclosures about the NSA have sparked a global debate about government surveillance and its impact on individual privacy.⁴ There is great interest in the United States and in Europe in having the revelations about the NSA serve as a catalyst for change in the way governments engage in surveillance to enhance national security. As some of you know, I have spent a lifetime working on privacy issues, so it should be no surprise that this is a debate I personally welcome, as my own view is that it is a conversation that is overdue.

But I also think it is important that we have the right conversation — one that is open and honest, practical and productive. As we move forward with this conversation, we should keep in mind that consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues. I and my colleagues at the FTC focus on the appropriate balance between consumer privacy interests and commercial firms' use of consumer data, not on national security issues. And I believe the recent revelations should spur a separate and equally long overdue conversation about how we can further enhance consumer privacy and increase transparency in the commercial sphere.

The FTC is the premier U.S. consumer protection agency focused on commercial privacy. The FTC has a great track record of using its authority to go after unfair or deceptive practices that violate consumer privacy, and vigorously enforcing other laws designed to protect financial⁵ and health⁶ information, information about children⁷, and credit information used to make decisions about credit, insurance, employment, and housing.⁸

³ See Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), available at <http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf>.

⁴ See Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (JUN. 9, 2013), available at <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

⁵ Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

⁶ Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. 300jj et seq. §§17901 et seq.

⁷ Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. We have brought enforcement actions against well-known companies, such as Google,⁹ Facebook,¹⁰ Twitter,¹¹ and Myspace.¹²

We have also brought myriad cases against companies that are not household names, but whose practices violated the law. We've sued companies that spammed consumers,¹³ installed spyware on computers,¹⁴ failed to secure consumers' personal information,¹⁵ deceptively tracked consumers online,¹⁶ violated children's privacy laws,¹⁷ inappropriately collected information on consumers' mobile devices,¹⁸ and failed to secure Internet-connected devices.¹⁹ We have obtained millions of dollars in penalties and restitution in our privacy and data security cases, and placed numerous companies under 20-year orders with robust injunctive provisions.

⁸ Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

⁹ In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* <http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf> (decision and order).

¹⁰ In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* <http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf> (decision and order).

¹¹ In the Matter of Twitter, Inc., FTC File No. 092 3093 (March 3, 2011) *available at* <http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf> (decision and order).

¹² In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* <http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf> (decision and order).

¹³ *See, e.g., FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* <http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf>.

¹⁴ *See, e.g., FTC v. CyberSpy Software, LLC, et al.*, No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* <http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf> (stipulated final order).

¹⁵ *See, e.g., In the Matter of LabMD*, FTC File No. 102 3099 (Aug. 28, 2013), *available at* <http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf> (administrative complaint).

¹⁶ *See, e.g., In the Matter of Epic Marketplace, Inc., et al.*, FTC File No. 112 3182 (Dec. 5, 2012), *available at* <http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf> (decision and order).

¹⁷ *See, e.g., U.S. v. Artist Arena, LLC*, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012), *available at* <http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf> (stipulated final order).

¹⁸ *See U.S. v. Path, Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), *available at* <http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf>; In the Matter of HTC, Inc., FTC File No. 122 3049 (June 25, 2013), *available at* <http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf> (decision and order).

¹⁹ *See In the Matter of TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013), *available at* <http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf> (agreement containing consent order); *see also* Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, *available at* <http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things>.

As a complement to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. In addition to our landmark privacy report issued last year, we have addressed cutting-edge privacy issues involving facial recognition technology,²⁰ kids apps,²¹ mobile privacy disclosures,²² and mobile payments.²³

In light of our increasingly interconnected world, the FTC has devoted significant time to enhancing international privacy enforcement cooperation so that we are better able to address global challenges. We continue to foster a strong relationship and engage in ongoing dialogue with European data protection authorities. We meet regularly with EU DPAs, and in April I met with the entire Article 29 Working Party. The Article 29 Working Party has been kind enough to recognize the FTC as a crucial partner in privacy and data protection enforcement.²⁴ And the Working Party, like the FTC, has welcomed the ongoing dialogue and constructive cooperation between us, and stressed the need for further transatlantic cooperation, especially in enforcement matters, in order to achieve our common goals.²⁵ Indeed, the FTC's recent Memorandum of Understanding with the Irish DPA establishes a good framework for increased, more streamlined, and more effective privacy enforcement cooperation.²⁶ And just last month, we worked very closely with our EU and Canadian counterparts to launch the International Conference of Data Protection and Privacy Commissioners' initiative to address challenges in global privacy enforcement cooperation.²⁷

²⁰ See Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at <http://ftc.gov/opa/2012/10/facialrecognition.shtm>.

²¹ See FED. TRADE COMM'N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf>.

²² See Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), available at <http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm>.

²³ See FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), available at <http://www.ftc.gov/os/2013/03/130306mobilereport.pdf>.

²⁴ Press Release, Article 29 Data Protection Working Party Meeting with FTC Commissioner Julie Brill (Apr. 29, 2013), available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130429_pr_april_plenary_en.pdf.

²⁵ See *Id.*

²⁶ Memorandum of Understanding Regarding Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, U.S. FED. TRADE COMM'N-DATA PROTECTION COMMISSIONER OF IRELAND, June 2013, available at <http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf>.

²⁷ See Resolution on International Enforcement and Cooperation, 35th International Conference of Data Protection and Privacy Commissioners, Sept. 23-26, 2013, available at <https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf>.

Another critical role played by the FTC is to enforce the U.S.-EU Safe Harbor framework.²⁸ We know that Safe Harbor has received its share of criticism, particularly in the past few months. We've read the news reports and heard about the recent Parliamentary hearings about Safe Harbor.²⁹ Given the active debate over Safe Harbor right now, I'd like to address head-on the contention in some quarters that Safe Harbor isn't up to the job of protecting EU citizens' data in the commercial sphere...

First, the FTC vigorously enforces the Safe Harbor. As the Safe Harbor program has grown over the past decade, so has the FTC's enforcement activity. Since 2009, we have brought ten Safe Harbor cases.³⁰ When Safe Harbor was established, the FTC committed to review on a priority basis all referrals from EU member state authorities.³¹ With few referrals over the past decade, we have taken the initiative to proactively look for Safe Harbor violations in every privacy and data security investigation we conduct. That is how we discovered the Safe Harbor violations of Google, Facebook, and Myspace in the last few years. These cases demonstrate the enforceability of Safe Harbor certifications and the high cost that companies can pay for non-compliance. The orders in Google, Facebook, and Myspace require the companies to implement comprehensive privacy programs and subject the companies to ongoing privacy audits for 20 years.³² Violations of these orders can result in hefty fines, as Google discovered when we assessed a \$22.5 million civil penalty against the company last year for violating its consent decree.³³ The FTC orders against Google, Facebook, and Myspace help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe. These cases demonstrate that Safe Harbor gives the FTC an effective and functioning tool to protect the privacy of EU citizen data transferred to America. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

Second, going forward, the FTC will continue to make the Safe Harbor a top enforcement priority. Indeed, we have opened numerous investigations into Safe Harbor compliance in recent months. We will continue to welcome any substantive leads, such as the complaint we received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations. And, let me be clear, we take this recent complaint very seriously. Of

²⁸ See U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), available at http://export.gov/safeharbor/eu/eg_main_018475.asp...

²⁹ See *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Sixth Hearing* (Oct. 7, 2013), available at <http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE...>

³⁰ See Legal Resources, Bureau of Consumer Protection Business Center, U.S. FED. TRADE COMM'N, available at <http://business.ftc.gov/legal-resources/2840/3...>

³¹ See Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n to John Mogg, Director, Directorate-General XV, European Commission (Jul. 14, 2000), available at http://export.gov/static/sh_en FTCLETTERFINAL Latest eg_main_018455.pdf...

³² See Google, *supra* note 9; Facebook, *supra* note 10; Myspace, *supra* note 12...

³³ See Press Release, Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), available at <http://ftc.gov/opa/2012/08/google.shtm>.

course, as we do in every instance, we take the necessary time to separate fact from fiction. And, as I am sure many in this audience would appreciate, we also proceed carefully to provide proper notice and appropriate levels of due process. If we discover in our investigations that companies have committed Safe Harbor-related law violations, we will take appropriate enforcement actions.....

As I mentioned earlier, I think it is healthy to have a vigorous debate over how to appropriately balance national security and privacy, but that ongoing debate should not be allowed to distort discussions in the commercial sphere about role of the Safe Harbor in protection consumer privacy. The EU itself has created national security exemptions in its existing data protection laws,³⁴ and the European Commission proposed such exemptions for government surveillance in its draft data protection regulation.³⁵ In other words, the EU has justifiably recognized the need to tackle their member states' national security issues separately. Safe Harbor is no different and warrants a similar approach. Just as the EU Data Protection Directive was not designed to address national security issues, neither was the Safe Harbor. Whatever the means to transfer data about European consumers for commercial purposes – whether to countries whose laws are deemed “adequate”, through approved contractual clauses, or by way of the Safe Harbor – all these transfer mechanisms are subject to national security exceptions. The difference is that, for Safe Harbor violations, the FTC is the cop on the beat. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection.

I know that some of you in this room may have taken a different view of the Safe Harbor framework. I hope my thoughts give you cause to reexamine the virtues of the Safe Harbor system. As the draft regulation continues its journey through the process of review and adoption, I am hopeful that we can continue to work together to promote both the free flow of data and strong consumer privacy protections.

And while it may not make the headlines or the nightly news, in the midst of all of the recent developments at home and across the pond, our efforts to enhance privacy enforcement cooperation continue to build trust day by day. We want to continue to develop these ties of cross border law enforcement cooperation – including Safe Harbor enforcement – that enhance privacy and data security – as these are the ties that build rather than erode trust, the ties that bind rather than divide us. We have worked extensively with our friends in the EU on these and other issues, and we look forward to continuing that collaboration to enhance privacy protection for consumers on both sides of the Atlantic.....

Thank you.....

³⁴ Directive 1995/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2005 O.J. (L 281) 31, 42, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

³⁵ See *Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

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

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

**[PROPOSED] ORDER GRANTING RESPONDENT’S MOTION TO DISQUALIFY
COMMISSIONER BRILL FROM THIS ADMINISTRATIVE PROCEEDING**

This matter came before the Commission on December 17, 2013, upon a Motion to Disqualify Commissioner Brill From This Administrative Proceeding (Motion) filed by Respondent LabMD, Inc. (LabMD) pursuant to Commission Rule 4.17, 16 C.F.R. § 4.17, for an Order disqualifying Commissioner Julie Brill from participation in the above-captioned matter. Having considered LabMD’s Motion and all supporting papers, and good cause appearing,

IT IS ORDERED THAT LabMD’s Motion **IS GRANTED;** and

IT IS FURTHER ORDERED THAT Commissioner Brill is disqualified from participating in the above-captioned matter, including but not limited to any vote concerning the above-captioned matter and the Commission’s forthcoming decision on LabMD’s pending Motion to Dismiss the Complaint with Prejudice.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED:

CERTIFICATE OF SERVICE

I hereby certify that on December 17, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

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

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

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

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

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

CERTIFICATE OF ELECTRONIC FILING

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

Dated: December 17, 2013


By 
Michael D. Pepson

EXHIBIT 2

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

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

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 black 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

DANIELLE E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL S. TURNER, OHIO
JOHN J. WHITMAN, JR., TENNESSEE
PATRICK T. MCCHESSY, NORTH CAROLINA
JIM GORDON, OHIO
JASON CHAFFETZ, UTAH
DIN WALTERS, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMARAL, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DEWINE, OHIO
TROY GOWDY, SOUTH CAROLINA
BEACON PATRICK, TEXAS
BOB HARTING, WASHINGTON
CYNTHIA A. LUMM, WYOMING
ROS WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK WATKINS, NORTH CAROLINA
KERRY L. BENNETT, MICHIGAN
RICK WARREN, CALIFORNIA

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 (205) 225-6974
Facsimile (202) 225-3874
Minority (202) 225-6081

<http://oversight.house.gov>

ELIJAH F. CUMMINGS, MARYLAND
RANKING MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN P. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPRIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TOMY CARDEAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

LAWRENCE 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.*

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

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/>

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

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

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/>

^[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/>.

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



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?

Duplicate



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.

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.

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





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

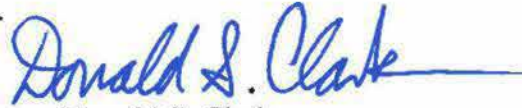
Finally, some of the information that could be discussed and documents to be provided could include internal staff analyses and recommendations, which are pre-decisional, deliberative information and materials exempt from mandatory public disclosure under FOIA Exemption 5, 5 U.S.C. § 552(b)(5). See *NLRB 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: 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



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

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

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

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

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

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.baiban@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

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

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?

Duplicate

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

Not an Agency Record

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.").

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.*

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) 225-5222
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.

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).



CIVIL INVESTIGATIVE DEMAND
Documentary Material

<p>1. TO</p> <p>The Privacy Institute C/O Jim Kelly or Rian Wroblewski 1 Regency Court Marlton, New Jersey 08053</p>	<p>2. FROM</p> <p>UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION</p>
--	---

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.

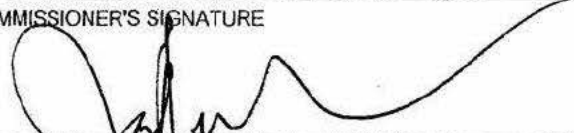
3. SUBJECT OF INVESTIGATION

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.

<p>4. DATE AND TIME MATERIAL MUST BE AVAILABLE</p> <p>AUG 13 2009</p>	<p>5. COMMISSION COUNSEL</p> <p>Alain Sheer, Division of Privacy and Identity Protection Federal Trade Commission 601 N.J. Ave. N.W. Washington, D.C. 20580 (202.326.3321)</p>
--	--

<p>6. RECORDS CUSTODIAN</p> <p>Alain Sheer, Division of Privacy and Identity Protection Federal Trade Commission 601 N.J. Ave. NW (Stop NJ 3158) Washington, D.C. 20580</p>	<p>7. DEPUTY RECORDS CUSTODIAN</p> <p>Katrina Blodgett, Division of Privacy and Identity Protection Federal Trade Commission 601 N.J. Ave. NW (Stop NJ 3158) Washington, D.C. 20580</p>
---	---

<p>DATE ISSUED</p> <p>7/10/09</p>	<p>COMMISSIONER'S SIGNATURE</p> 
-----------------------------------	--

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.

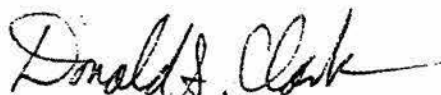
The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation.

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.



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Alan Sheer
Attorney
Division of Privacy and Identity Protection

Direct Dial: 202.326.3324
Fax: 202.326.3629
E-mail: asheer@ftc.gov

January 19, 2010

Via Federal Express

Michael J. Daugherty
LabMD, Inc.
2030 Power Ferrys Road
Bldg. 500, Suite 520
Atlanta, GA 30339

Dear Mr. Daugherty:

As I discussed today with Mr. Boyle, the staff of the Federal Trade Commission ("Commission") is conducting a non-public inquiry into LabMD, Inc.'s compliance with federal law governing information security. According to information we have received, a computer file (or files) from your computer network is available to users on a peer-to-peer file sharing ("P2P") network (hereinafter, "P2P breach").¹ The file (or files) contains sensitive information about consumers and/or employees that could be used to commit identity theft or fraud or cause other types of harms to consumers and/or employees.²

Section 5 of the FTC Act prohibits deceptive or unfair acts or practices, such as misrepresentations about privacy and security and practices that cause substantial injury to

¹ P2P networks are created when users install compatible peer-to-peer file sharing applications on personal computers in homes and businesses. The applications link these computers together and can be used to share files between the computers. Once a file has been shared, the original source of the file cannot remove the file from the P2P networks or control access to it by other users on the networks.

For information about security concerns raised by the use of peer-to-peer file sharing applications and possible responses to them, see the enclosed *Peer-to-Peer File Sharing: A Guide For Business*, www.ftc.gov/bep/edu/pubs/business/idtheft/bus16.shtm.

² One such file is *insuranceaging 6.05.071*.

consumers.³ Accordingly, we seek to determine whether your handling of sensitive information from or about consumers and/or employees raises any issues under Section 5.

We invite you to meet with us in our Washington, D.C. office to discuss this matter, or to discuss this matter with us by telephone. If possible, we would like to meet during the week of March 8, 2010. In advance of the meeting, we request that you provide us with the information and documents listed below by February 22, 2010. Please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. Any materials you submit in response to this request, and any additional information that you mark "Confidential," will be given confidential treatment.⁴

In preparing your response:

- Please provide all responsive documents in the possession, custody, or control of LabMD, and its parents, owners, subsidiaries, divisions, affiliates, branches, joint ventures, and agents (collectively, "LabMD", "you," or "your").
- Please submit complete copies of all documents requested, even if you deem only part of a document to be responsive.
- Responses to each request should describe in detail each material change or update that has been made that concerns, refers, or relates to the request, as well as the date the change or update was implemented and the reason(s) for the change or update.
- Please number each page of your response by Bates stamp or otherwise, and itemize your response according to the numbered paragraphs in this letter.
- If any document is undated, please indicate in your response the stamped page numbers of the document and the date on which you prepared or received it.
- If you do not have documents that are responsive to a particular request, please submit a written statement in response. If a document provides only a partial response, please submit a written statement which, together with the document, provides a complete response.
- If you decide to withhold responsive material for any reason, including an applicable privilege or judicial order, please notify us before the date set for

³ 15 U.S.C. § 45 *et seq.*

⁴ The Commission's procedures concerning public disclosure and confidential treatment can be found at 15 U.S.C. §§ 46(f) and 57b-2, and at Commission Rules 4.10 - 4.11 (16 C.F.R. §§ 4.10 - 4.11).

responding to this request and submit a list of the items withheld and the reasons for withholding each.

- Please do not submit documents that contain any individual consumer's or employee's date of birth, Social Security number, driver's license or other personal identification number, financial account information, or medical information. If you have responsive documents that include such information, please redact the information before providing the documents.
- We may seek additional information from you at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested below, but also any other information that concerns, reflects, or relates to this matter, including files and information stored electronically, whether on computers, computer disks and tapes, or otherwise) until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.⁵ This request is not subject to the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.
- A responsible corporate officer or manager of LabMD shall sign the responses and certify that the documents produced and responses given are complete and accurate.
- For purposes of this letter, the term "personal information" means individually identifiable information from or about an individual consumer, including, but not limited to: (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) telephone number; (e) date of birth; (f) government-issued identification number, such as a driver's license, military identification, passport, or Social Security number, or other personal identification number; (g) financial information, including but not limited to: investment account information; income tax information; insurance policy information; checking account information; and credit, debit, and/or check-cashing card information, including card number, expiration date, security number (such as card verification value), information stored on the magnetic stripe of the card, and personal identification number; (h) health information, including, but not limited to: prescription medication and dosage; prescribing physician name, address, and telephone number; health insurer name, and insurance account and policy numbers; and medical condition or diagnosis; (i) employment information, including, but not limited to, income, employment, retirement, disability, and medical records; (j) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is

⁵ Failure to retain documents that may be relevant to this matter may result in civil or criminal liability. 15 U.S.C. § 50.

combined with other available data that identifies an individual consumer; or (k) any information from or about an individual consumer that is combined with any of (a) through (j) above. For the purpose of this definition, an individual consumer shall include an "employee", and "employee" shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under your control.

REQUESTS FOR DOCUMENTS AND INFORMATION

Please provide the documents and information identified below.⁶ Unless otherwise indicated, the time period covered by these requests is from January 1, 2007 through the date of full and complete production of the documents and information requested.

General Information

1. Identify the complete legal name of LabMD and all other names under which it does, or has done, business, its corporate mailing address, and the date and state of incorporation.
2. Identify and describe LabMD's parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, and entities over which it exercises supervision or control. For each such entity, describe in detail the nature of its relationship to LabMD.
3. Identify each individual or entity having an ownership interest in LabMD, as well as their individual ownership stakes and their positions and responsibilities within LabMD.
4. Provide documents sufficient to describe your business in detail. The response should identify and describe: each product and service you offer; each location (both online and offline) through which you offer such products and services; and, annually, your revenue, number of employees, and number of customers.

Personal Information

5. Provide documents that describe in detail the types of personal information you collect.

⁶ For purposes of this letter: the word "any" shall be construed to include the word "all," and the word "all" shall be construed to include the word "any;" the word "or" shall be construed to include the word "and," and the word "and" shall be construed to include the word "or;" the word "each" shall be construed to include the word "every," and the word "every" shall be construed to include the word "each;" and the term "document" means any preexisting written or pictorial material of any kind, regardless of the medium in which such material was created, and regardless of the method by which it is stored (e.g., computer file, computer disk or tape, microfiche, etc.).

obtain, store, maintain, process, transmit, handle, or otherwise use (collectively, "collect and store") in conducting your business, how and where you collect and store the information, and how you use the information. The response should include, but not be limited to: documents sufficient to identify the type(s) of personal information you collect and store, the source(s) of each such type of information (such as consumers, employees, medical providers, healthcare plans, and insurance companies), and the manner by which you collect or obtain the information (such as by paper documents or electronically through a website); and documents or a narrative that describe in detail how you use each type of information in conducting your business.

Security Practices

6. Identify by name, location, and operating system each computer network that you use directly or indirectly to collect and store personal information, and provide for each such network:
 - (a) a high-level diagram (or diagrams) that sets out the components of the network and a narrative that describes the components in detail and explains their functions and how they operate together on the network. The description of the network components should identify and locate (within the network): computers; servers; firewalls; routers; internet, private line, and other connections; connections to other internal and external networks; virtual private networks; remote access equipment (such as wireless access points); websites; and security mechanisms and devices (such as intrusion detection systems). In responding, please feel free to use blueprints and diagrams that set out in detail the components, topology, and architecture of the network;
 - (b) documents sufficient to identify each computer, server, or other device where you collect and store personal information and, for each such computer, server, or device, each program, application, or other means (collectively, "databases") used to collect and store personal information; and
 - (c) documents that concern, relate, or refer to each database identified in the response to Request 6(b), including, but not limited to: operating manuals; user guides; communications with database vendors; database schemes, diagrams, and/or blueprints (including table and field names); and documents sufficient to identify the length of time for which you maintain personal information in the database.
7. Provide documents or a narrative that describe in detail the flow path of personal information over each network identified in response to Request 6, including the initial collection point for personal information (such as a website), the entry and exit points to and from the network, and all intermediate points within the network.
8. Provide documents sufficient to identify the policies, procedures, and practices you have used on each network identified in the response to Request 6 to prevent unauthorized

access to personal information collected and stored on the network, as well as the time period during which such policies, procedures, and practices were written and implemented. The response should include, but not be limited to, documents that concern, reflect, or relate to: controls on direct or remote access to personal information (such as a firewall policy or a password policy); controls on accessing and/or downloading personal information without authorization; the lifecycle of personal information, including maintaining, storing, using, and/or destroying the information; controls on the installation of programs or applications on computers or work stations on the network by employees or others; limits on the transmission of personal information within the network and between the network and other (internal or external) networks; logging network activity and reviewing the logs; secure application and website development; employee training; and plans for responding to security incidents.

9. For each network identified in the response to Request 6, provide documents that describe in detail each security policy, procedure, practice, control, defense, or other measure (collectively, "security practice") used on the network. The response should include, but not be limited to:
- (a) all documents that concern, reflect, or relate to each security practice, including, but not limited to, practices to control the installation and/or use of P2P programs (whether such programs are authorized or not);
 - (b) documents that set out the technical configurations of devices and programs you use to enforce each security practice, including, but not limited to, the configurations of firewalls or other means used to control or block P2P communications to and from the network and networks that connect to it;
 - (c) training or security awareness materials provided to network users (such as employees and third-party persons and entities with access to the network) regarding your security practices, such as materials that concern security generally or the use of and risks presented by P2P programs;
 - (d) documents that set out the frequency and extent to which such network users receive training or security awareness materials generally and as to the use of and risks presented by P2P programs;
 - (e) documents sufficient to identify by name and title each employee who is, or has been, responsible for coordinating security practices on the network, and to describe the responsibilities of each such employee;
 - (f) documents sufficient to identify whether and, if so, when you conducted or obtained (from another person or entity) a risk assessment to identify risks to the security, integrity, and confidentiality of personal information on the network;
 - (g) all documents that concern, reflect, or relate to testing, monitoring, and/or

evaluations of the effectiveness of security practices used on the network, including the dates when such activities were conducted and completed and plans and procedures for future testing, monitoring, and/or evaluation of security practices; and

- (h) documents that set out in detail all changes made to security practices on the network based upon testing, monitoring, and/or evaluations identified in the response to Request 9(g).
10. Provide all documents that concern, reflect, or relate to each risk assessment identified in the response to Request 9(f) and the security risks identified therein, if any. For each such assessment, the response should include, but not be limited to:
- (a) documents sufficient to identify the date of the assessment and the name and title of the person(s) responsible for conducting the assessment;
 - (b) a copy of the assessment;
 - (c) documents that describe in detail the steps taken in conducting the assessment;
 - (d) documents that concern, reflect, or relate to specific risks identified in the assessment and how you addressed each such risk; and
 - (e) a copy of each (internal or external) report or other document that verifies, confirms, challenges, questions, or otherwise concerns the assessment.
11. Provide documents sufficient to identify each third-party person or entity that, in the course of providing services to you ("service provider"), receives, maintains, processes, or otherwise is permitted access to personal information collected and stored by you.
12. For each service provider identified in the response to Request 11, provide:
- (a) documents sufficient to identify the types of personal information to which the service provider has access;
 - (b) documents sufficient to describe the manner and form of the service provider's access to personal information (such as physical access to your offices, remote access to your computer network(s), or the mailing of paper documents or computer storage media);
 - (c) a narrative that explains in detail the business reasons why the service provider has access to such information;
 - (d) copies of all contracts between you and the service provider;

- (e) documents that describe in detail the measures you took to select and retain the service provider to ensure that it is capable of appropriately protecting personal information you have provided or made available to the service provider; and
- (f) documents that describe in detail how you monitor the service provider to confirm that it has implemented and maintained security measures adequate to protect the security, integrity, and confidentiality of such personal information.

Other Information

- 13. Provide documents sufficient to identify any instance of which you are aware (including, if appropriate, the P2P breach) where personal information from a network identified in the response to Request 6 was or may have been shared or accessed without authorization (the "intrusion"), and, for each such intrusion, identify when and how you first learned about the intrusion, the network(s) involved, and all persons with knowledge about it.
- 14. Separately for each intrusion identified in the response to Request 13, provide all documents prepared by or for you that identify, describe, investigate, evaluate, or assess:
 - (a) how the intrusion occurred;
 - (b) the time period over which it occurred;
 - (c) the security vulnerabilities that were or may have been exploited in the intrusion;
 - (d) the actual or suspected point of entry;
 - (e) the path the intruder followed from the (actual or suspected) point of entry to the location of the personal information that was or may have been compromised and then in exporting or downloading the information (including all intermediate points);
 - (f) the type(s) and amount(s) of personal information that was or may have been accessed without authorization; and
 - (g) the security measures you implemented in response to the intrusion.

Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in the intrusion; (formal and informal) security audits or forensic analyses of the intrusion prepared internally and by third parties; security scans (such as for packet capture tools, password harvesting tools, rootkits, P2P programs, and unauthorized programs); incident reports; documents that identify the intruder; logs that record the intruder's steps in whole or part in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of reviews by

network administrators or others of logs and warnings; records setting out the routine security activities and checklists performed by network administrators (such as verifying that scheduled jobs were authorized); and other documents that concern, reflect, or relate to the intrusion, such as minutes or notes of meetings attended by you or your employees.

15. Separately for each intrusion identified in the response to Request 13 that was accomplished or facilitated by a P2P program and for the P2P breach if not identified in the response to Request 13 ("collectively, "P2P intrusion"), identify each P2P program (including version number and upgrade) that was, or may have been, used in any way in the intrusion. For each such program:

- (a) identify: the manufacturer, model, type, operating system, and network location of each computer or other electronic device on which the P2P program was installed (collectively, the "breach computer"); the source from which the program was downloaded to the breach computer; when and by whom the program was downloaded and installed on the breach computer; when the program was removed from the breach computer; how long the program was active on the computer; whether the default settings on the program were changed after it was installed on the breach computer, and, if so, when, by whom, and in what ways; and whether you authorized the installation and use of the program on the breach computer;
- (b) explain in detail your business need for using the program, if any, and identify who was using the program and why they were using it;
- (c) explain in detail all limitations you placed on use of the program, including security practices; and
- (d) provide a copy of each file generated as a result of installing the program on the breach computer, including, but not limited to, executable, history, and configuration files.

16. Separately for each P2P intrusion:

- (a) provide all logs, audits, assessments, or reports that concern, reflect, or relate to the intrusion;
- (b) identify the name of each folder and subfolder that was shared (uploaded or downloaded) through the intrusion, the name (including file extension) and content of each internal and external file (other than a purely music or video file) that was shared, and the amount and type of personal information in each file that was shared; and
- (c) describe in detail each folder, subfolder, file, and/or program (including functionality) that was shared through the intrusion.

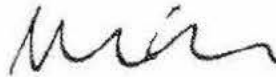
17. Separately for each intrusion identified in the response to Request 13, provide all documents that concern, relate, or refer to fraud and/or identity theft attributable to the intrusion and to the consequences of the fraud or identity theft. Responsive documents should include, but not be limited to:
- (a) fraud reports, alerts, or warnings issued by bank associations, banks, or other entities; documents that assess, identify, evaluate, estimate, or predict the number of consumers or employees that have, or are likely to, suffer fraud or identity theft; claims made against you for fraud or identity theft, such as by affidavits filed by consumers or employees; and documents that assess, identify, evaluate, estimate, or predict the dollar amount of fraud, identity theft, or other costs (such as for increased fraud monitoring or providing fraud insurance) attributable to the intrusion;
 - (b) documents that concern, reflect, or relate to investigations of or complaints filed with or against you relating to the intrusion, including, but not limited to, private lawsuits, correspondence with you, and documents filed with Federal, State, or local government agencies, Federal or State courts, and Better Business Bureaus; and
 - (c) documents or a narrative that identifies how (such as by public announcement or individual breach notification letter), when, how many, and by whom consumers and/or employees were notified that their personal information was or may have been obtained without authorization through the intrusion. If notification has been made, explain why notification was made (*e.g.*, compelled by law) and provide a copy of each substantively different notification. If notification was not provided as soon as you became aware of the intrusion or was not provided to all affected consumers and/or employees or at all, provide a narrative explaining why not.
18. Provide documents sufficient to identify all policies, claims, and statements you have made regarding the collection, disclosure, use, storage, destruction, and protection of personal information, including any policies, claims, or statements relating to how you secure personal information, and for each such policy, claim, or statement identify the date(s) when it was adopted or made, to whom it was distributed, and all means by which it was distributed.

Please send all documents and information to: Alain Sheer, Division of Privacy and Identity Protection, Federal Trade Commission, 600 Pennsylvania Ave., NW, Mail Stop NJ-8122, Washington, D.C. 20580. Due to extensive delays resulting from security measures taken to ensure the safety of items sent via the U.S. Postal Service, we would appreciate receiving these materials via Federal Express or a similar delivery service provider, if possible.

Thank you for your prompt attention to this matter. Please contact me (at 202.326.3321)

if you have any questions about this request or need any additional information.⁷

Sincerely,



Alain Sheer
Division of Privacy and Identity Protection

⁷ The Commission 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 Commission strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

EXHIBIT 3

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

ONE HUNDRED THIRTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MICHELY, 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
OOC 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

December 1, 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 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.*

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.

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



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	
<p>On 4/18/2008, 1 file was detected being disclosed by what appears to be a potential provider of services for CIGNA.</p> <p>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.</p> <p>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.</p>	

TIVERSA – CUSTOMER RESTRICTED

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



Forensic Investigation Report for Ticket #CIG00081

August 12, 2008

CONFIDENTIAL

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

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. 2 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 didn't.

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.

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.



Forensic Investigation Report - LABMD0001

Prepared for LabMD

1.0 Introduction

Worldwide Peer-to-Peer ("P2P") file sharing networks are primarily used for sharing music, movies, and software. Unfortunately, they also commonly expose confidential and sensitive government, corporate and consumer documents. Employees, suppliers, contractors, agents, partners, and customers inadvertently disclose millions of confidential and sensitive documents on the P2P file sharing networks each year.

Once disclosed, these documents are publicly available to any individual using one of the 2,800+ different P2P file sharing programs and versions, most of which are free and publicly available. Disclosed files are routinely accessed by identity thieves, cyber criminals, terrorists, competitors, the media, shareholders, and others.

It must be emphasized that P2P file sharing networks are not part of the World Wide Web. P2P file sharing networks are entirely separate, internet-based networks with unique searches, files, and users. P2P networks are extremely large. In fact, more users search the P2P for information than the World Wide Web, with over 1.8 billion searches a day occurring on the P2P networks. It is also estimated that over 550 million users have file sharing applications, and internet service providers have stated that up to 70% of internet traffic is consumed solely by P2P networks.

The risks related to P2P compromises will only escalate as P2P use continues to grow – driven by increased broadband access, the explosion of digital content, and increasing numbers of tech-savvy individuals entering the workforce. From a data and information security standpoint, P2P compromises are among the most damaging since users unknowingly share hundreds of documents, sometimes every file resident on their machine, including Word, Excel, PowerPoint, PDF, e-mails, databases, and PST files. Once these documents are shared or exposed to the millions of P2P users, they tend to "virally spread" across the networks as users continuously download these files from each other and thereafter proceed to re-share these files themselves.

Tiversa's unique value is in its patented EagleVision X1™ technology which can view and access the P2P in real-time. Similar to how Google has indexed the World Wide Web, Tiversa has "centralized" the notoriously "decentralized" P2P file sharing networks. As such, Tiversa has the ability to 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, and remediate P2P file disclosures.

This Forensic Investigation Report summarizes the results and suggested actions of Tiversa's Forensic Investigation Services for Incident LABMD0001.

SECTION 1 - Customer Information

Organization Name	N/A
Contact Name	N/A
Contact Phone	N/A
Contact Email	N/A

SECTION 2 - Incident Information

Incident Number	LABMD0001
Related Incidents	N/A
Date of Report	6/4/2014
Severity	URGENT

SECTION 3 - Preliminary Disclosure Information

IP Address	64.190.82.42
P2P Client	N/A
Disclosure Type	Internal
Disclosure Source	LabMD
Filename(s)	insuranceaging_6.05.071.pdf

SECTION 4 - Incident Summary

On 2/5/2008, Tiversa's systems detected 1 file being disclosed on P2P file sharing networks. The detected file appears to be a 1,718 page "Insurance Aging" Report relating to "LABMD. INCORPORATED." The file contains patient information including Name, Social Security Number, DOB, Insurance Information, Billing Date Code/CPT, Billed Amount etc., relating to approximately 9,000 apparent patients.

The file appears to be emanating from the IP Address 64.190.82.42, which traces to Atlanta, Georgia, US.

Upon further analysis, 19 total files were detected being disclosed from this IP address on various dates between 3/7/2007 and 2/25/2008. The additional files include Insurance Benefits labels, LabMD login credentials (username and passwords) relating to web access for insurance companies, LabMD Insurance Verification Specialist Duties, blank forms relating to daily credit card transactions, LabMD Medical Records Request letters, LabMD Patient Appeal Authorization letters, LabMD Payment Posting Specialist Duties, a LabMD Employee Handbook, LabMD Employee Time Off Request forms, documents containing meeting notes and other related letters.

Upon reviewing the metadata and files emanating from this source, Tiversa believes the disclosure source may be an individual employed with LabMD.

2.0 Investigation Findings

2.1 Source Identification

The disclosure source appears to have emanated from IP address 64.190.82.42. As of 6/3/2014 this IP address is registered to CYPRESSCOM.NET (CYPRESS COMMUNICATIONS LLC), and appears to be located in Atlanta, Georgia, US. For details related to this IP address see Figure 2-1-1 below.

Figure 2-1-1:
Disclosure Source IP Address/ Geolocation

IP Address	64.190.82.42
Location	 UNITED STATES, GEORGIA, ATLANTA
Latitude & Longitude	33.831847, -84.386614 (33°49'55"N 84°23'12"W)
Connection	CYPRESS COMMUNICATIONS LLC
Local Time	03 Jun, 2014 05:41 PM (UTC -04:00)
Domain	CYPRESSCOM.NET

Based on an initial investigation by Tiversa, the information found within the content and metadata of the files disclosed by this source indicate that the disclosure source may be an individual employed with LabMD.

There were 19 total files disclosed by this source. The file metadata (properties) of several of the documents list authoring *Company* as "lab md," and contain the following common identifiers within the file *Author* and *Last-Saved by* fields:

rwoodson
sbrown
Administrator
Dan Carmichael
LabMD
Liz Fair

It is possible that these are user identifiers, providing additional evidence in that these users may have created or edited the disclosed documents, and that the documents may have been created or edited on a LabMD machine. See Figure 2-1-2 below for all file information.

Figure 2-1-2:
Disclosure Source IP Address - 64.190.82.42

File Title	Disclosure Date	Company	Author	Last Saved by
INSURANCE BENEFITS LABELS.doc	3/7/2007		Liz Fair	sbrown
WEB ACCESS FOR INSURANCE COMPANIES.doc	3/7/2007	LabMD		sbrown
LabMD Insurance Verification Specialist Duties.doc	3/7/2007		sbrown	sbrown
HELPFUL TIPS FOR BETTER AUDIT RESULTS.doc	3/15/2007		sbrown	sbrown
DAILY CREDIT CARD TRANSACTIONS.doc	10/11/2007		sbrown	sbrown
MEDICAL RECORDS FEE LTR.doc	11/10/2007	labmd	Administrator	sbrown
MEDICAL RECORDS RELEASE.doc	11/10/2007	labmd	Administrator	sbrown
MEDICAL RECORDS REQ LTR.doc	11/10/2007	labmd	Administrator	rwoodson
PATIENT APPEAL AUTHORIZATION LTR.doc	11/10/2007	labmd	Administrator	rwoodson
LabMD Payment Posting Specialist Duties.doc	11/10/2007		sbrown	rwoodson
Patient Locator Project.doc	11/13/2007		rwoodson	rwoodson
Humana patient Doc.doc	11/13/2007	labmd	rwoodson	rwoodson
Employee Handbbook.doc	11/15/2007		Dan Carmichael	
Employee Application Benefits.pdf	11/15/2007		a498584	
Employee Time Off Requests2007.doc	11/29/2007		rwoodson	rwoodson
insuranceaging_6.05.071.pdf	2/5/2008			
BCBS HMO & POS APPEAL LTR.doc	2/25/2008	labmd	Administrator	rwoodson
BCBS PAID PT LTR.doc	2/25/2008	labmd	Administrator	rwoodson
Roz's Coverage.doc	2/25/2008		rwoodson	rwoodson

One file emanating from this source appears to be a letter from the following individual:

*Rosalind Woodson
Billing Manager/LabMD
rwoodson@labmd.org*

This individual appears to be employed with LabMD and may have utilized the "rwoodson" user identifier as referenced within the metadata of the disclosed documents.

One of the additional files emanating from this source appears to be a Medical Records Request letter from the following individual:

Sandra Brown
Billing Manager/LabMD
*(678) 443-2338 *Direct**
sbrown@labmd.org

This individual appears to be employed with LabMD and may have utilized the "sbrown" user identifier as referenced within the metadata of the disclosed documents.

Given these findings, it is possible that Rosalind Woodson or Sandra Brown may have disclosed the documents utilizing a P2P file sharing application from a work or home computer. It should be noted that the 1,718 page "Insurance Aging" Report (*insuranceaging_6.05.071.pdf*) was detected being disclosed on P2P file sharing networks on 2/5/2008. A total of 19 files were detected being disclosed on P2P file sharing networks between 3/7/2007 - 2/25/2008 from the IP Address 64.190.82.42.

See Figure 2-1-3 below for a sample of redacted screenshots of the documents emanating from this source.

Figure 2-1-3:

Insurance Aging

LABMD, INCORPORATED

LABMD

Report Options
6/5/2007 12:07:11PM

Option	Value
Age From	06/05/2007
Show Billing History	All dates Billed
Sort Insurance By	Insurance Code
Show Summary Only	No
Show Billing Detail	Yes
Subtotal by Billing	No
Subtotal by Provider	Yes

Insurance Aging

LABMD, INCORPORATED

LABMD

HUMANA P O BOX 14601, LEXINGTON, KY 40233 (502) 580-5650

JOSEF
 Insurance: Primary ID: _____ Date of Birth: _____ Insured: Self

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total
Patient Total:										

CLAUDETTE
 Insurance: Primary Group Number: _____ ID: _____ Date of Birth: _____ Insured: Self

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total
Patient Total:										
Insurance Total:										

TRICARE PO BOX 7890, MADISON, WI 53707 (800) 403-3950

TOMMY
 Insurance: Secondary ID: _____ Date of Birth: _____ Insured: Self

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total
Patient Total										

Printed 6/5/2007 12:07:11PM Page 1718 of 1718

Figure 2-1-4:



1117 Perimeter Center West, Suite #W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 968-8743 * Fax (678) 443-2329

October 19, 2006

James [REDACTED]

RE: Authorization to Appeal Insurance Denial

Insured's ID#: [REDACTED]

Group #: [REDACTED]

Date of Service: 5/19/2006

Total Charge: \$110.00

Dear Mr. [REDACTED]

Blue Cross/Blue Shield has denied our claim for your laboratory services due to non-network participation.

LabMD applied for an in-network contract with prior to your date of service, however, it was not approved until 12/19/2005. *Your urologist, [REDACTED] does not have any knowledge of the contract between LabMD and Blue Cross/Blue Shield, as this contract deals specifically with laboratory/pathology services and fee schedules, so please direct all questions or comments to [REDACTED] at LabMD.

Author:	Administrator
Manager:	
Company:	labmd

Last saved by:	rwoodson
Revision number:	21
Total editing time:	747 Minutes

Figure 2-1-5:

WEB ACCESS FOR INSURANCE COMPANIES

BCBS FL (Not Available)

BCBS GA (www.bcbsga.com)

USER NAME: [REDACTED]

PASSWORD: [REDACTED]

BCBS SC (www.southcarolinablues.com)

USER NAME: [REDACTED]

PASSWORD: [REDACTED]

BCBS TN (www.bcbst.com)

USER NAME: [REDACTED]

PASSWORD: [REDACTED]

HUMANA (www.humana.com)

USER NAME: [REDACTED]

PASSWORD: [REDACTED]

Author: LabMD

Manager:

Company:

Last saved by: sbrown

Revision number: 4

Total editing time: 20 Minutes

Figure 2-1-6:

The image shows a document titled "LabMD Employee Handbook". The title "LabMD" is in large red font, and "Employee Handbook" is in a smaller, italicized black font below it. To the left of the title, there is a "Welcome to LabMD," section. Below that is a paragraph of text explaining the handbook's purpose and stating that it does not create an employment contract. On the right side, there is a metadata box with the following information:

Author:	Dan Carmichael
Manager:	
Company:	
Last saved by:	rwoodson
Revision number:	2
Total editing time:	1 Minute

Figure 2-1-7:

LabMD Payment Posting Specialist Duties

INSURANCE PAYMENT POSTING

1. Posting Specialist will post insurance payments (correlate with Explanation of Benefits, including "no-pay" denials) from daily batches in [REDACTED]
2. After each insurance batch is posted, Posting Specialist will run "Day Sheet-Transaction Detail Report" to make sure payments posted in [REDACTED] "balance"/equals insurance deposit tape total.
 - a. Select "Reports" from Toolbar at Main Menu in [REDACTED]
 - b. Select "Day Sheet".
 - c. Under Options Tab, unclick "Subtotal by Provider" and
 - d. Select "Sort by Name".

Author:	sbrown
Manager:	
Company:	

Last saved by:	rwoodson
Revision number:	3
Total editing time:	34 Minutes

Figure 2-1-8:

LabMD
THE LABORATORY SERVICES COMPANY
1117 Perimeter Center West, Suite #W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 967-8743 * Fax (678) 443-2329

March 13, 2006

RE: [REDACTED]
DOB: [REDACTED]
SS #: [REDACTED]
ACCT #: [REDACTED]
DOS: [REDACTED]

To Whom It May Concern:

[REDACTED]

If you have any further questions, do not hesitate to contact our office at (678) 443-2330, Monday through Friday, between 8am-6pm EST.

Sincerely,

Sandra Brown
Billing Manager/LabMD
(678) 443-2338 *Direct*
sbrown@labmd.org

Author:	Administrator
Manager:	
Company:	labmd
Last saved by:	sbrown
Revision number:	4
Total editing time:	11 Minutes

Figure 2-1-9:



1117 Perimeter Center West, Suite #W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 967-8743 * Fax (678) 443-2329

March 23, 2007

[Redacted text]

To Whom It May Concern:

This letter serves as a formal request to have claims for the attached list of patients reprocessed

If you have any further questions, do not hesitate to contact me directly at (678) 443-2338, Monday through Friday, between 8am - 6pm.

Sincerely,

Rosalind Woodson
Billing Manager/LabMD
rwoodson@labmd.org

Author:	Administrator
Manager:	
Company:	labmd

Last saved by:	rwoodson
Revision number:	6
Total editing time:	20 Minutes

2.2 File Spread Analysis

In addition to the above disclosure source identification and geolocation analysis, Tiversa also performed a file spread analysis to determine if any of the LabMD-related files have spread, and were acquired by any other users of P2P networks. Based on this analysis, Tiversa detected (6) additional IP addresses disclosing one or more of the files originally detected emanating from 64.190.82.42.

See Figure 2-2-1 below for a summary table of all IP addresses detected.

Figure 2-2-1:
File Spread Analysis – IP Summary Table

Source#	IP Address	Disclosure Date(s)	ISP	Geolocation**	Total Files
Source 1	64.190.82.42*	3/7/2007 - 2/25/2008	CYPRESS COMMUNICATIONS LLC	ATLANTA, GEORGIA, US	19
Source 2	68.107.85.250	2/5/2008 - 9/20/2011	COX COMMUNICATIONS INC.	SAN DIEGO, CALIFORNIA, US	3,302
Source 3	173.16.83.112	11/5/2008 - 2/14/2009	MEDIA COM COMMUNICATIONS CORP	CHICAGO, ILLINOIS, US	1,832
Source 4	201.194.118.82	4/7/2011	SAN JOSE (SANJOSECA.GOV)	SAN JOSE SAN JOSE, CR	33
Source 5	90.215.200.56	6/9/2011	EASYNET LTD	LONDON, ENGLAND, UK	47
Source 6	71.59.18.187	5/5/2010 - 11/7/2012	COMCAST CABLE COMMUNICATIONS HOLDINGS INC	ALPHARETTA, GEORGIA, US	254
Source 7	173.16.148.85	2/23/2009 - 11/7/2012	MEDIA COM COMMUNICATIONS CORP	NASHVILLE, TENNESSEE US	520

*Indicates original disclosure source IP reported in Incident LABMD0001

**All IP Geolocation information associated with these IP addresses was discovered as of 6/3/2014.

The 6 additional IP addresses were detected in possession of the 1,718 page "Insurance Aging" Report (*insuranceaging_6.05.071.pdf*) on various dates within the disclosure date ranges referenced above.

These 6 IP addresses possess additional files including federal tax returns relating to numerous individuals, credit reports, credit card and bank account statements, passports, usernames and passwords to online accounts, medical payment data, lists of credit card numbers, social security numbers, instructions on how to hack and steal passwords etc. Tiversa classifies these 6 additional IP addresses as Information Concentrators.

Throughout our extensive P2P research, Tiversa continues to see individuals harvesting a large number of files containing confidential and sensitive data. Tiversa calls these individuals "Information Concentrators" and in most cases, they are suspicious in nature. These individuals utilize P2P file sharing networks to search for sensitive and confidential data (i.e. Credit Card #'s, Passwords, Account #'s, SSN, PII, Payroll Information, HR, Medical, Financial, IT Information etc). Information Concentrators gather this information and could potentially use it for malicious purposes.

For a complete list of file titles detected in possession of these additional IP addresses, see the excel file titled "LABMD0001_Forensic_Investigation_Report_File_Spread_Analysis.xls", which is provided along with this report.

3. Conclusions/Suggested Actions

In order to contain any further proliferation of these LabMD-related files across the P2P networks, any computers responsible for their disclosure must be identified and then removed from the P2P networks – or at a minimum, the LabMD related files must be removed from the suspect's machine.

Based on the information reviewed by Tiversa, a suggested course of action is to contact the apparent LabMD employees listed within the Investigation findings above (Rosalind Woodson and Sandra Brown) reference the disclosed document titles, document content, and the supporting evidence listed above. It is possible that an investigation into these disclosed files and possible sources will allow LabMD to determine the disclosure source. If the disclosure source machine is found, the machine should be reviewed for the presence of file sharing software. An investigation of this machine should indicate that the files found on that machine match the file listing noted in Figure 2-1-2 above. It should be noted that the disclosure source machine may be a home computer, work computer or possibly a laptop.

Additional remediation activities can be discussed with Tiversa once additional investigation steps by LabMD have been completed.



Tiversa
606 Liberty Avenue
Pittsburgh, PA 15222

(724) 940-9030 *office*
(724) 940-9033 *fax*

www.tiversa.com

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

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

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

**[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.'S
MOTION TO DISQUALIFY COMMISSIONER EDITH RAMIREZ**

This matter came before the Commission on April 27, 2015, upon a Motion to Disqualify Commissioner Edith Ramirez From This Administrative Proceeding (Motion) filed by Respondent LabMD, Inc. (LabMD) pursuant to Commission Rule 4.17, 16 C.F.R. § 4.17, for an Order disqualifying Commissioner Edith Ramirez from participation in the above-captioned matter. Having considered LabMD's Motion and the entire Record in this matter,

IT IS ORDERED that Respondent LabMD, Inc.'s Motion to Disqualify Commissioner Edith Ramirez be and the same is hereby GRANTED; and

IT IS FURTHER ORDERED THAT Commissioner Ramirez is disqualified from participating in the above-captioned matter, including but not limited to any vote concerning the above-captioned matter.

Donald S. Clark
Secretary

SEAL
ISSUED:

CERTIFICATE OF SERVICE

I hereby certify that on April 27, 2015, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

I certify that on **April 28, 2015**, I caused hand-delivery of twelve paper copies of the foregoing document to the following address: Document Processing Unit, RFO Receiving Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610, Washington, DC 20024.

I also certify that on April 27, 2015, 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 on April 27, 2015, 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

CERTIFICATE OF ELECTRONIC FILING

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

Dated: April 27, 2015

By: /s/ Patrick J. Massari