UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: EDITH RAMIREZ, CHAIRWOMAN
MAUREEN K. OHLHAUSEN
TERRELL MCSWEENY

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

RESPONDENT LabMD, INC.'S OPPOSITION TO COMPLAINT COUNSEL'S MOTION FOR LEAVE TO FILE SURREPLY

Respondent LabMD, Inc. ("LabMD") hereby opposes Complaint Counsel's ("CC") Motion for Leave to File Surreply ("CC Motion").

ARGUMENT

I. A PASSING REMARK EXPRESSING A GOOD-FAITH BELIEF IN A FOOTNOTE DOES NOT JUSTIFY A SURREPLY

CC primarily seeks to file a surreply because it takes issue with the following isolated statement in *a footnote* of LabMD's Reply: "Mr. Sheer's draconian obsession with destroying LabMD culminated in his importuning Tiversa to provide fraudulent evidence of 'spread' regarding the 1718 File."[1] *See* CC Proposed Surreply at 2 (quoting LabMD Reply at 1 n.2). CC's

[1] This is consistent with far more detailed allegations set forth in a public (and publicized) *Bivens* lawsuit against Mr. Sheer in his individual capacity currently pending in the U.S. District Court for the District of Columbia. *See* Compl. ¶¶ 1, 94-102, *LabMD et al. v. Sheer et al.*, No. 1:15-cv-02034-TSC, Dkt. 1 (D.D.C. Nov. 20, 2015)(attached as Exhibit A). LabMD's *Bivens* lawsuit has received media attention. *See, e.g.,* Joe Van Acker, "LabMD Sues 3 FTC Lawyers Over Data Security Case," LAW360 (Nov. 24, 2015), http://www.law360.com/articles/731134/labmd-sues-3-ftc-lawyers-over-data-security-case. LabMD's *Bivens* Complaint is also publicly available. *See, e.g., id.* CC is evidently aware of this lawsuit. *See* CC Stay Opposition at 9 n.9.

Motion and Proposed Surreply should be rejected, because CC misinterprets the foregoing footnote's passing observation and fails to acknowledge that the record in this case and publicly-available information justify it. Most importantly, however, CC's Motion fails to explain how this footnote raises any issue that would justify a surreply under Rule 3.22(d).

Rule 3.22(d) allows for a surreply only where a party wishes to draw the Commission's attention to "recent important developments or controlling authority that could not have been raised earlier in the party's principal brief." While CC may take issue with LabMD's word choice, CC acknowledges in the very filing at issue here that LabMD has made "allegations regarding the character, motives, and conduct" of Alain Sheer "throughout this litigation." CC Proposed Surreply at 1. Nor did CC identify any controlling authority that could not have been raised before. CC's Motion to file a surreply to challenge a footnote has no basis in the Rules, nor does it present any argument relevant to LabMD's stay application.

Moreover, the record in this case and publicly-available information is replete with facts justifying the footnote. CC focuses on *Mr. Wallace's* testimony alone, mistakenly concluding that that is the sole reason for LabMD's suspicions. *See* CC Proposed Surreply at 2-3. Not so.

To be sure, Mr. Wallace's testimony confirms that which the Commission Opinion acknowledges: "The ALJ found...that after the meeting between Tiversa and FTC staff in the fall of 2009, Mr. Boback directed Mr. Wallace to generate false information purporting to show that the 1718 file had spread...." Op. 32 n.84. Mr. Wallace testified that Alain Sheer was present at this meeting. Tr. 1385-1388. The ALJ found Mr. Wallace's testimony credible. IDF 155.

But LabMD is not solely relying on this (which is why Mr. Wallace's testimony is not cited in support). Likewise, LabMD is not exclusively relying on record evidence (which is why no record evidence is cited). Rather, LabMD has a good-faith belief that should LabMD choose to

request and should the Court of Appeals allow LabMD to take discovery that it was denied in the administrative case—but which may be available now, *see* 15 U.S.C. § 45(c); *FTC v. Std. Oil Co.*, 449 U.S. 232, 244-46 (1980)—LabMD would be able to uncover evidence necessary to establish the full extent of Mr. Sheer's interactions with Tiversa. Put simply, there is evidence to justify LabMD's good-faith belief that Mr. Sheer[2] did, in fact, "importune"[3] Tiversa to provide fraudulent "spread" evidence, enabling LabMD to prove that assertion with direct evidence.

LabMD has already specifically (and publicly) alleged this in great detail in a currently pending *Bivens* action against, among others, Mr. Sheer in his individual capacity.[4] *See* Compl.

---

[2] LabMD's Counsel is *not suggesting here* that other members of CC's trial team were involved in or aware of conduct LabMD has a good-faith basis to believe occurred in certain Tiversa-FTC meetings and related phone conversations. This distinction has been drawn elsewhere. For example, Mr. Sheer is the only member of CC's trial team who is a defendant in the *Bivens* action.

[3] This would not necessarily have involved an express request and could be implicit. *See, e.g., Tully v. Del Re*, No. 00-C-2829, 2002 U.S. Dist. LEXIS 18840, *9-14 (N.D. Ill. Oct. 1, 2002) (involving allegations that police officers implicitly importuned informant to manufacture false basis for criminal charge, "making it clear to her (though perhaps without directly saying so) that they wanted evidence against Tully no matter what she had to do to manufacture it" and then "knew, or recklessly disregarded, that the information…[provided by the informant] was false").

[4] Particularly because the ALJ quashed LabMD's deposition subpoena to Sheer and effectively barred LabMD from obtaining discovery on FTC staff's precomplaint investigation, LabMD's suspicions about Sheer's interactions with Tiversa have not been dispelled. This is no different whatsoever from LabMD's able counsel in the *Bivens* lawsuit, who pleaded on information and belief that Sheer and others "agreed and conspired" that Boback and Tiversa would provide false evidence of spread. *See* Compl. ¶¶ 1, 94-102, *LabMD et al. v. Sheer et al.* LabMD was denied discovery on FTC staff's precomplaint investigation early in the case—well before Mr. Wallace revealed that CC's case was predicated on false evidence. *See* Exhibit B (ALJ orders barring discovery into pre-complaint investigation). The ALJ found that "limiting Respondent's discovery… [in this way] does not prejudice Respondent's ability to pursue at a later phase of the case its claim that the Commission's actions in investigating and filing the Complaint were unlawful." Order Granting Complaint Counsel's Motion to Quash and To Limit Deposition Subpoenas Served on Commission Attorneys, 7 n.4 (Feb. 25, 2014) (citing *Standard Oil.*, 449 U.S. at 245-46). This is that later phase of this case.

¶¶ 1, 94-102, *LabMD et al. v. Sheer et al.*, No. 1:15-cv-02034-TSC, Dkt. 1 (D.D.C. Nov. 20, 2015) (attached as Exhibit A). For example, LabMD's *Bivens* Complaint avers: "On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would provide the FTC false evidence of source and spread." *Id.* ¶ 97. Similarly, it alleges "Sheer knew…CX0019 was fraudulent but proceeded with the evidence anyway,"[5] *id.* ¶ 146; and, Tiversa committed criminal felony HIPAA violations when it stole and transferred LabMD's 1718 File to FTC, *see id.* ¶¶ 13-14, 49. The *Bivens* Complaint further avers that Sheer and FTC committed criminal HIPAA violations[6] when they knowingly procured the 1718 File, and subsequently bamboozled the Commission into issuing its LabMD Complaint, *see id.* ¶¶ 106, 133-134; and "[o]n information and belief, Sheer…misrepresented material facts to the Commission," *id.* ¶ 124.

Moreover, questions raised by a congressional report addressing, *inter alia*, the FTC's relationship with Tiversa suggest a good-faith basis for the footnote statement. *See* STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113TH CONG., TIVERSA, INC.: WHITE KNIGHT OR HIGH-TECH PROTECTION RACKET (2015) (the "OGR Report").[7] The OGR Report found:

- Boback testified that "the only person I 'know' at the FTC is Mr. Sheer." OGR Report at 55 n.162.

---

[5] CX0019 is Tiversa's fabricated "spread" evidence. *See* IDF146-154. *In 2009*, Tiversa/Privacy Institute produced to Sheer a spreadsheet indicating the 1718 File was found at *one* IP address: 64.190.82.42; *in 2013*, Tiversa produced CX0019, which lists *four* completely different IP addresses at which Tiversa then claimed to have found the 1718 File. *Compare* CX0307, *with* CX0019. Sheer relied on CX0019 anyway. *See* Tr. 16-17.

[6] *See* LabMD FOF at ¶¶ 217-220.

[7] The OGR Report is attached as Exhibit 35 to LabMD's Stay Application (RX644).

- "According to Boback, Sheer contacted him after the July 2009 Oversight hearing to set up a visit to Tiversa. A second contact occurred when Sheer visited Tiversa in August 2009." *Id.* 55.
- "Boback met with Sheer for the third time in Washington, D.C., after the Privacy Institute responded to the FTC's CID with information it in turn obtained from Tiversa...." *Id.* ("Sheer in particular did not recall meeting with Tiversa in Washington, D.C." *Id.* 56.)
- "FTC told the Committee that it had limited contact with Tiversa....E-mails produced to the Committee...show a much more cooperative relationship between Tiversa and the FTC." *Id.*
- "Personnel from the FTC's Division of Privacy and Identity Protection told the Committee that Tiversa's contacts with...FTC prior to the July 2009 hearing took place with a different division of...FTC. Yet, Alain Sheer was included on e-mails with Boback requesting information about a recent Tiversa press release and scheduling the March 5, 2009, conference call[.]" *Id.* 57.
- "[I]n the four months leading up to the July 2009 Oversight Committee hearing, ***Tiversa employees called Alain Sheer at his FTC office on 21 occasions***." *Id.* (emphasis added).
- "Regular phone calls between Tiversa and...FTC took place between August 2009, when Tiversa provided information to...FTC, and January 19, 2010, when...FTC sent letters to nearly all of the companies Tiversa turned over to...FTC. ***During these months, Tiversa employees called Alain Sheer 34 times***.... FTC represented to the

Committee that only a handful of phone calls ever took place....The phone records stand in stark contrast to this assessment." *Id.* 57-58 (emphasis added).

- "Troublingly, despite Tiversa's close relationship with Lifelock, a company that was itself the subject of an FTC investigation, Sheer stated that he was unaware of the relationship between Lifelock and Tiversa before being informed of it by Committee staff in a transcribed interview.... ***FTC used Tiversa as the source of convenient information used to initiate enforcement actions....*** " *Id.* 67 (emphasis added).
- "Evidence produced to the Committee shows that...FTC notified Tiversa of its investigatory schedule, so that Tiversa knew when the Commission would issue complaint letters and act accordingly." *Id.* 71.[8]

The OGR Report further indicates that LabMD has been denied access to sufficient information to fully understand Tiversa's relationship with Mr. Sheer.[9] For example, it contains Sections titled:

- "Tiversa's Relationship with the Federal Trade Commission";

---

[8] Tiversa's former CEO, Robert Boback, has now invoked his Fifth Amendment rights. *See* LabMD Stay Application at 4 n.3; Daugherty Decl., Exs. A-B. He is the *second* Tiversa operative to do so in connection with Tiversa's dealings with the FTC regarding the 1718 File. That speaks for itself. Interestingly, a recent FTC OIG Semiannual Report to Congress states: "Allegation that the FTC Disseminated False Data. The OIG...[was] ask[ed] to investigate alleged collaboration between the FTC and a company suspected of disseminating false data about data security breaches. In particular, ... whether the FTC had used false data in an enforcement action against another company. The OIG did not substantiate the allegations...." FTC, OIG Semiannual Report to Congress: 04.01.15-09.30.14, at 10 (Oct. 31, 2015), https://www.ftc.gov/system/files/documents/reports/fiscal-year-2015-second-half/semi1554.pdf. The subject(s) of this OIG investigation have not been revealed. Regardless of what the FTC OIG allegedly found, whether CC "used" Tiversa's false evidence after Wallace's testimony is different from whether Sheer importuned its creation.

[9] OGR had access to documents, materials, and testimony that LabMD did not. For example, OGR was able to interview Sheer; LabMD was not, because the ALJ quashed its subpoena to Sheer.

- "Tiversa misrepresented the extent of its relationship with the FTC to the Committee";
- "The FTC misrepresented the extent of its relationship with Tiversa to the Committee";
- "The FTC failed to question Tiversa's creation of a dubious shell organization, the Privacy Institute, to funnel information to the FTC"; and
- "Tiversa manipulated advanced, non-public, knowledge of FTC regulatory actions for profit."

OGR Report at 2; *see id.* at 53-72. *Cf.* IDF100-168 (detailed factual findings on Tiversa and its role in the FTC investigation and administrative prosecution of LabMD). Should a Court of Appeals order additional discovery, *see* 15 U.S.C. § 45(c); *Std. Oil Co.*, 449 U.S. at 244-46, there is reason to believe that LabMD may obtain direct evidence proving that Mr. Sheer implicitly or explicitly encouraged Tiversa to provide false evidence against LabMD.

CC's Motion to file a surreply pertaining to a footnote should be denied because it lacks basis in Rule 3.22(d) and because the footnote has a good-faith basis as supported by the record and publicly-available information.

II. LABMD'S SUPPLEMENTAL DECLARATION IS PROPER

CC argues that Mr. Daugherty's Supplemental Declaration is improper because "the substance of Respondent's evidence regarding Part I compliance costs was not addressed in Complaint Counsel's Opposition" to LabMD's stay application. *See* Proposed Surreply at 3-4. Based on this factual claim, CC argues that Mr. Daugherty's declaration violates Rule 3.56(c), 16 C.F.R. § 3.56(c), which states that a reply must be "limited to new matters raised by the answer." *See* CC Proposed Surreply at 4.

The factual predicate for CC's argument is incorrect. CC's Opposition states:

> Respondent contends that establishing and implementing a comprehensive information security program, *as required by Part I of the Order*, would impose

> substantial costs, but provides no factual support for this assertion. First, Respondent claims that even attempting to adopt a comprehensive information security program would require consulting with and paying Information Technology ("IT") professionals and attorneys. Daugherty Decl. ¶ 22(a)(iv). *However, Respondent has failed to quantify or otherwise provide any specific facts regarding the costs associated with these activities. In light of the limited nature and scope of Respondent's current operations, the Commission cannot presume, without appropriate quantification and supporting evidence, that such expenses would be substantial.*

CC Stay Opposition at 10 (emphasis added).

Mr. Daugherty's Supplemental Declaration primarily addressed the foregoing statements, which CC made in its Opposition regarding LabMD's alleged inability to adequately substantiate its estimates of compliance costs associated with Part I of the Final Order. *See* Supp. Daugherty Decl. ¶¶ 2, 5-10. Therefore, it is proper because it specifically responds to matters raised by CC's Stay Opposition.[10] This is true *a fortiori* because it was CC that apparently implied that LabMD should (and needed to) provide additional factual support in the form of "appropriate quantification and supporting evidence"[11]—which LabMD did. Thus, CC's argument fails.

CONCLUSION

For these reasons, CC's Motion should be DENIED and CC's proposed Surreply should be STRICKEN.

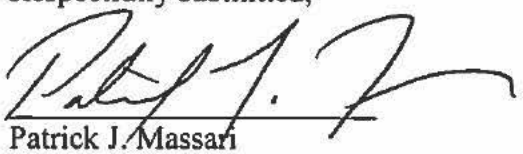
---

[10] Mr. Baker's Declaration addresses his data-security qualifications and is part of the record on review. *See* 16 C.F.R. § 3.43(i).

[11] LabMD submitted sufficient evidence in support of its Stay Application. However, to dispel any doubt and assuage CC's apparent concern, LabMD provided additional support in its Reply. Rule 3.56(c) does not bar LabMD from doing this.

Dated: September 21, 2016

Respectfully submitted,



Patrick J. Massari
Erica L. Marshall
Cause of Action Institute
1875 Eye Street, NW Suite 800
Washington, DC 20006
Phone: (202) 499-4232
Facsimile: (202) 330-5842
Email: patrick.massari@causeofaction.org

Counsel for Respondent, LabMD, Inc.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **EDITH RAMIREZ, CHAIRWOMAN**
MAUREEN K. OHLHAUSEN
TERRELL MCSWEENY

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

[PROPOSED] ORDER DENYING COMPLAINT COUNSEL'S MOTION FOR LEAVE TO FILE SURREPLY

Having considered Complaint Counsel's Motion for Leave to File Surreply and all supporting and opposition papers,

IT IS ORDERED that Complaint Counsel's Motion for Leave to File a Surreply is DENIED and that Complaint Counsel's proposed Surreply is hereby STRICKEN FROM THE RECORD.

ORDERED:

By the Commission.

Donald S. Clark
Secretary

SEAL ISSUED:

CERTIFICATE OF SERVICE

I hereby certify that on September 21, 2016, I caused to be filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send an electronic notification of such filing to the Office of the Secretary:

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

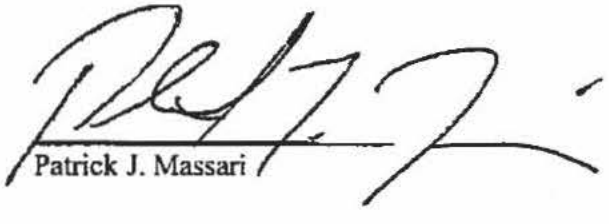
I also certify that I delivered via hand delivery and electronic mail copies of the foregoing document to:

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

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

Alain Sheer, Esq.
Laura Riposo Van Druff, 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., NW
Room CC-8232
Washington, DC 20580

Dated: September 21, 2016



Patrick J. Massari

CERTIFICATE OF ELECTRONIC FILING

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

Dated: September 21, 2016

Patrick J. Massari

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL J. DAUGHERTY
[redacted]

and

LABMD, INC.
[redacted]

Plaintiffs,

v.

ALAIN H. SHEER
(in his individual capacity)
[redacted]

and

RUTH T. YODAIKEN
(in her individual capacity)
[redacted]

and

CARL H. SETTLEMYER, III
(in his individual capacity)
[redacted]

and

DOES 1-10
(in their individual capacities),

Defendants.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Michael J. Daugherty ("Daugherty") and LabMD, Inc. ("LabMD") (collectively, Daugherty and LabMD are referred to as "Plaintiffs"), by and through counsel, bring this action against Defendants Alain H. Sheer ("Sheer") in his individual capacity; Ruth T. Yodaiken ("Yodaiken") in her individual capacity; Carl H. Settlemyer, III ("Settlemyer") in his individual capacity; and Does 1-10, in their individual capacities (collectively, Sheer, Yodaiken, Settlemyer and Does 1-10 are referred to as "Federal Defendants"), and allege the following:

NATURE OF THE CASE

1. This *Bivens* action is based on an FTC investigation and prosecution fought so aggressively, abusively, unethically and illegally by FTC attorneys Sheer, Yodaiken and Settlemyer that they put a small cancer-detection firm in Atlanta, Georgia out of business. They did so without *any* incriminating evidence and by withholding exculpatory evidence not only from the targets of their investigation but also from responsible members of the FTC staff and FTC Commissioners who, based on the defendants lies and omissions, granted them authority to proceed with their illegal and unconstitutional pursuits. Every step of the way, the defendant FTC attorneys supported their actions with lies, thievery and testimony from a private company, Tiversa, whose business model was based on convincing companies to pay them to "recover" files that, in truth, *they* hacked from computers all over the world. The defendant FTC attorneys here knew or should have known from the very start of their investigation that their evidence and their arguments about unfair practices and impending consumer harm were fictional. These defendants gathered and relied upon stolen property, perjured testimony, documents from a sham organization and a company now known for stealing documents and lying about there whereabouts, all in the alleged interest of protecting consumers from unfair practices.

PARTIES

2. Daugherty, a resident and citizen of the state of Georgia, is over 18 years of age.

3. LabMD is a corporation organized and existing under the laws of the state of Georgia. Its principal place of business is located in Fulton County, Georgia. Daugherty is the sole owner of LabMD and is its president and chief executive officer.

4. Sheer is a resident and citizen of the state of Maryland, is over 18 years of age and can be served with process at [redacted], or wherever he may be found. At all times relevant to this Complaint, Sheer has been an attorney employed by the Federal Trade Commission (the "FTC").

5. Yodaiken is a resident and citizen of the state of Maryland, is over 18 years of age and can be served with process at [redacted], or wherever she may be found. At all times relevant to this Complaint, Yodaiken has been an attorney employed by the FTC.

6. Settlemyer is a resident and citizen of the state of Virginia, is over 18 years of age and can be served with process at [redacted], or wherever he may be found. At all times relevant to this Complaint, Settlemyer has been an attorney employed by the FTC.

JURISDICTION AND VENUE

7. This Court has jurisdiction under 28 U.S.C. § 1331 and 28 U.S.C. § 1343. This case arises under the Constitution and laws of the United States of America. Daugherty and LabMD bring this action for damages against Federal Defendants named in their individual capacities, under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).

8. This Court has personal jurisdiction over the Federal Defendants because a substantial portion of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

9. Venue is proper in this District and this Division pursuant to 28 U.S.C. § 1391.

FACTUAL BACKGROUND

10. From at least 2001 through approximately January 2014, LabMD operated as a small, medical services company providing doctors with cancer-detection services.

11. In connection with its testing and other services, LabMD collected and maintained certain personal information on thousands of patients ("Personal Information"). For purposes of this Complaint, 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." Personally Identifiable Information ("PII") is a subset of the data in Personal Information, including a person's name, address, date of birth, Social Security number, credit card and banking information, and drivers' license number.

12. Personal Information collected and maintained by LabMD includes information protected by privacy requirements set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). LabMD has at all times complied with HIPAA.

13. Various state and federal laws prohibit the unauthorized taking, possession and disclosure of PII and Personal Information. *See, e.g.,* 42 U.S.C. § 1320d-6(a)(2) (criminal violations for obtaining individually identifiable health information relating to an individual and/or disclosing individually identifiable health information to another person);

14. Various state and federal laws prohibit hacking of computers to obtain information and documentation, including PII and Personal Information. *See, e.g.*, O.C.G.A. §16-9- 93 (criminal violations for computer theft, computer trespass, computer invasion of privacy, or computer forgery).

15. Tiversa Holding Corp. ("Tiversa") is a privately held company headquartered in Pittsburgh, Pennsylvania. Tiversa was founded by Robert Boback ("Boback") and Samuel Hopkins ("Hopkins") in January 2004.

16. Hopkins, a high-school dropout, left Tiversa in 2011.

17. Prior to joining Tiversa, Boback was a practicing chiropractor who dabbled in various activities such as buying and selling residential properties and selling cars on eBay.

18. At all times relevant to this Complaint, Boback has been the chief executive officer of Tiversa.

Tiversa

19. Tiversa is a data security company that offers breach detection and remediation services. Tiversa uses a combination of off-the-shelf and proprietary technology purportedly to search entire peer-to-peer networks for documents of interest to its customers or potential customers and downloads the documents it finds into its data storage devices. Tiversa has claimed that it "provides P2P intelligence services to corporations, government agencies and

individuals based on patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day."

20. Tiversa searches for and downloads data from peer-to-peer networks. The data is kept in what is referred to as Tiversa's "data store" ("Data Store"). The Data Store contains files that Tiversa has downloaded from peer-to-peer networks. The Data Store also contains information as to where the downloaded files had been located.

21. Tiversa does not seek permission to access computers or download files from computer workstations, even though it knows that much of what it finds and downloads to its Data Store are files that were never intended to be shared.

22. Tiversa's business model is to capitalize on finding and downloading files that were never intended to be shared. Thus, Tiversa is particularly interested in finding and downloading items such as individual and corporate tax returns, medical records, social security numbers, credit card numbers, passwords, employment records, trade secrets, privileged and protected information, military and other state secrets, PII and Personal Information. Tiversa collects such files without permission or authority, even though there are state and federal laws designed to prevent this kind of information gathering and storage.

23. Tiversa purports to be a white knight in the world of inadvertent file sharing.

24. The amount of inadvertently shared files searched for, located and stored by Tiversa is massive.

25. Boback has testified to Congress that Tiversa downloads "the equivalent of the Library of Congress every three days."

26. Tiversa claims to be able to see entire peer-to-peer networks, instead of a smaller subset as seen by an individual user.

27. There are two ways for data to get into Tiversa's Data Store: (1) Tiversa's proprietary program, Eagle Vision, automatically downloads files returned from Tiversa's automated searches and (2) Tiversa's forensic analysts insert data that the analysts find using a stand-alone computer running a peer-to-peer client (*e.g.*, LimeWire).

28. In Tiversa's searches for exposed files on peer-to-peer networks, Tiversa records in its Data Store (1) the information disclosed, (2) the IP address of the disclosing computer, (3) metadata from the file, (4) the identity of the disclosing company and (5) when the information was disclosed. Much of this information is included on spreadsheets that Tiversa analysts update several times a day. The purpose of the spreadsheets is so that Boback and the Tiversa sales force can make sales calls to the affected companies.

29. When contacting the affected company to sell services, Tiversa's practice was to not reveal the source of the information and to tell the potential customer that Tiversa had not recorded the IP information. Tiversa would provide the found documents to the potential customer only after stripping the IP address and removing any metadata relating to the disclosure source, while keeping a separate set of the files that included disclosure source information.

30. Tiversa monetizes information it obtains from peer-to-peer networks either by selling a monitoring contract (pursuant to which Tiversa would search for certain key words for a period of time), or by selling a "one-off" service (which would remediate just the existing disclosure problem). Tiversa typically creates an "incident response" for its "one-off" services.

31. Tiversa often fabricates information and documentation regarding the disclosing source of files it finds on peer-to-peer networks. If a potential customer would not purchase Tiversa's services, Tiversa would often attempt to monetize peer-to-peer network findings by

notifying an *existing* Tiversa customer of the source of the customer's information and advising the *existing* customer to contact Tiversa's target.

32. When a company refused to purchase Tiversa's services, Boback would often tell his analysts, in reference to that company, to the effect of, "you think you have a problem now, you just wait." In many of these situations, Boback directed Tiversa analysts to input information into Tiversa's Data Store so as to make that company's information "proliferate" and thereby make it appear, fraudulently, that a file had "spread" to multiple places. Tiversa would then use this "evidence" to follow up with a company to try again to get the company to purchase Tiversa's remediation services.

33. For companies that initially refused to purchase Tiversa's services, Tiversa would often follow up with the target by stating, fraudulently, that the disclosed document had spread to additional IP addresses, including IP addresses of known "bad actors" or identity thieves. In such cases, Tiversa's analysts would alter or create source and spread information in the Data Store to make it appear that Tiversa had located and downloaded the file from the IP address of a known bad actor and that files had proliferated on peer-to-peer networks.

34. Starting as early as 2006, Tiversa created an Advisory Board whose members came to include General Wesley K. Clark (retired general of the United States Army; former candidate for President of the United States of America); Maynard Webb (former chief operating officer for eBay); Dr. Larry Ponemon (chairman and founder of the Ponemon Institute); Howard Schmidt (former Chief Security Strategist for the U.S. CERT Partners Program for the National Cyber Security Division, Department of Homeland Security and former Vice President and Chief Information Security Officer and Chief Security Strategist for eBay); Michael Dearing (former Senior Vice President & General Merchandise Manager for eBay); Thomas Keeven (former Vice

President of Infrastructure, Vice President of Operations and Vice President of Architecture for eBay); Lynn Reedy (former Chief Technical Officer and Senior Vice President of Product & Technology for eBay) and Patrick Gross (a founder and former chairman of the executive committee of American Management Systems, Inc.).

35. On July 24, 2007, Boback testified in a hearing before the U.S. House of Representatives Committee on Oversight and Government Reform (the "Oversight Committee") on the topic of inadvertent file sharing over peer-to-peer networks.

36. Tiversa Advisory Board member Wesley Clark also testified at that hearing, immediately after Boback. Among other statements, General Clark testified as follows:

> I want to just disclose now that I am an advisor to Tiversa, and in that role I do have a small equity stake in Tiversa. But my engagement here has just opened my eyes to activities that I think, if you saw the scope of the risk, I think you would agree that it is just totally unacceptable. The American people would be outraged if they were aware of what is inadvertently shared by Government agencies on P2P networks. They would demand solutions.
>
> As I was preparing for the testimony, I asked Mr. Boback to search for anything marked classified secret, or secret no-foreign. So he pulled up over 200 classified documents in a few hours running his search engine. These documents were everything from in sums of what is going on in Iraq to contractor data on radio frequency information to defeat improvised explosive devices. This material was all secret, it was all legitimate.
>
> Even more alarming, I got a call from Bob Boback on Wednesday night that he had found on the peer-to-peer net the entire Pentagon's secret backbone network infrastructure diagram, including the server and IP addresses, with password transcripts for Pentagon's secret network servers, the Department of Defense employees' contact information, secure sockets layer instructions, and certificates allowing access to the disclosing contractors' IT systems, and ironically, a letter from OMB which explicitly talks about the risks associated with P2P file-sharing networks. So I called the Office of the Secretary of Defense. I got the right people involved. They had some meetings on it this. It turns out that a woman with top-secret clearance working for a contractor on her home computer, she did have LimeWire, and somehow, I guess, she had taken some material home to work on it, and so all this was out there.
>
> But these two examples illustrate the risks that are out there. Peer-to-peer file sharing is a wonderful tool. It is going to be a continuing part of the economy. It is a way that successfully moves large volumes of data, and that is not going to go away, but it has to

> be regulated and people have to be warned about the risks, and especially our Government agencies - our National Security Agency, DOD, people that run the Sipranet - have to take the appropriate precautions, because we can't have this kind of information bleeding out over the peer-to-peer network.

37. Boback and General Clark's testimonies caught members of Congress and several federal agencies off guard. Tiversa, Boback and General Clark appeared to have more insight, more actual examples, more evidence, more technological capabilities, more expertise and more awareness of the problems of inadvertent file sharing on peer-to-peer networks than those in the federal government who believed this issue was their responsibility, including the Federal Trade Commission.

Tiversa and the FTC Agree to Cooperate

38. Boback, Settlemyer and other FTC staff members began communicating approximately two months after the 2007 Congressional hearing on inadvertent file sharing. These communications were as frequent as weekly during some periods. The subject matter of these communications was information available on peer-to-peer networks.

39. Boback believed he could capitalize on Tiversa's newfound arrangement with the FTC by reporting to the FTC companies that refused Tiversa's services, the expected result of which was that those companies would respond to FTC inquiries by hiring Tiversa.

40. The FTC intended to capitalize on its relationship with Tiversa by using Tiversa's technological capabilities and expertise to identify targets for investigations and prosecutions and by using evidence obtained from Tiversa to prosecute.

41. In the fall of 2007 or winter of 2007/2008, members of the FTC staff visited Boback at Tiversa's facility in Pennsylvania. Following that meeting, the FTC began requesting that Tiversa provide information to the FTC. Tiversa, Settlemyer and other members of the FTC

staff essentially agreed that, in the world of cybersecurity, Tiversa would be the FTC's stalking horse.

Peer-to Peer Networks

42. In peer-to-peer networks, computer files (*e.g.*, music, videos and pictures) can be shared directly between computers connected to one another via the internet.

43. Peer-to-peer file-sharing applications (*e.g.*, LimeWire) enable one computer user to make a request to search for all files that have been made available for sharing by another computer user, so long as the other computer is also using the file-sharing application.

44. Users of peer-to-peer networks perform searches using terms related to the particular file they hope to find and receive a list of possible matches. The user then chooses a file they want to download from the list.

45. The search capabilities on peer-to-peer networks are limited. For example, peer-to-peer networks are only capable of searching for filenames. These networks do not have the capability for users to search for files using words or other data contained *in* the files that have been made available for sharing by other users. In addition, search terms must be precise. With LimeWire, for example, a user searching for files with the search terms "insurance" and "aging" would not find any insurance aging files with the filename "insuranceaging."

46. A document being "shared" or "made available for sharing" on a peer-to-peer network is available to be downloaded by another computer user on the same peer-to-peer network. The fact that a document is being shared, or made available for sharing does not mean the document has been "downloaded" for viewing or is immediately viewable. The contents of a file that is available for sharing are not disclosed until the file is downloaded and viewed by the requesting user.

47. In many cases, files that are "shared" on a peer-to-peer network are shared without the knowledge of the user of a computer that has a file sharing application on it. The user may not even know that the computer he or she is using has a file sharing application. Such situations are often referred to as "inadvertent file sharing via P2P networks." Considerable research has been done and papers written on the topic. *See, e.g.,* "Filesharing Programs and "Technological Features to Induce Users to Share,"" A Report to the United States Patent and Trademark Office from the Office of International Relations, Prepared by Thomas D. Sydnor II, John Knight and Lee A. Hollaar (November 2006).

Tiversa's Theft of LabMD's Property

48. In May 2008, Tiversa targeted LabMD as a potential customer. Tiversa contacted LabMD to inform it that a LabMD file containing Personal Information was available through LimeWire. This particular file was a 1,718-page PDF document containing Personal Information on approximately 9,300 patients (the "1718 File"). The 1718 File was victim of inadvertent file sharing.

49. In truth, Tiversa had, without any authority, accessed and downloaded ("hacked") the 1718 File from a LabMD billing computer in Atlanta, Georgia on February 25, 2008. Tiversa's unauthorized download and retention of Personal Information was a violation of several state and federal crimes.

50. The filename on the document Tiversa hacked was "insuranceaging_6.05.071.pdf". The chance that anyone would ever have searched for or found the 1718 file was extremely remote. In order for Tiversa to receive a search result for the "insuranceaging_6.05.071.pdf" file, it would have to have searched for the document using the highly unusual search terms "insuranceaging" or "6.05.071".

51. Only Tiversa, with its "patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day" and its cadre of highly experienced professional hackers, would ever have found the 1718 File.

Tiversa's Lies to LabMD

52. Immediately after Tiversa's call, LabMD investigated and determined that the 1718 File was inadvertently available because, unbeknownst to LabMD, LimeWire was installed on a LabMD billing computer. LabMD determined within minutes that LimeWire was installed on only one of its computers and removed the LimeWire application right away.

53. As part of LabMD's investigation regarding the 1718 File, LabMD employees constantly searched peer-to-peer networks for the 1718 File until 2013. Those employees were never able to find the 1718 file on any peer-to-peer network.

54. Soon after Tiversa first contacted LabMD in May 2008, it began a series of efforts to convince LabMD to purchase its remediation services. These efforts continued from mid-May through mid-July 2008.

55. During these sales efforts, Tiversa told LabMD that its patented technology and forensic experts had determined that the 1718 File was being searched for on peer-to-peer networks and that the 1718 File had spread across peer-to-peer networks. Except to the extent Tiversa observed LabMD employees searching for the 1718 file, these were lies.

56. On May 13, 2008, a Tiversa analyst specifically told LabMD the following:

- "our system shows a record of continued availability for sporadic periods over the past several months but we did not attempt to download it again."
- "The system did not auto-record the IP, unfortunately, most likely due to the little amount of criteria indexed against the DSP. "

- "The actual source IP address in the data store logs [is] not readily available at this point. If it is there, I should be able to get it but it would take some time."

These were lies.

57. On May 22, 2008, Tiversa told LabMD, "We have continued to see people searching for the file in question on the P2P network by searching precisely for the exact file name of the file in question. They may or may not have been successful in downloading the file however." Except to the extent Tiversa observed LabMD employees searching for the 1718 file, these were lies.

58. On July 15, 2008, Tiversa told LabMD that it "continued to see individuals searching for and downloading copies of the [1718 File]." This was a lie. No one was downloading copies of the 1718 File because it was not available for sharing on any peer-to-peer network.

59. On July 22, 2008, LabMD instructed Tiversa to direct any further communications to LabMD's lawyer.

60. Tiversa's sales tactics became even more aggressive. On November 21, 2008, Jim Cook, one of Tiversa's attorneys, told an attorney for LabMD that he had been talking to the FTC about LabMD. Cook justified his actions by claiming that Tiversa was concerned about being sued for having knowledge of the "breach" and not reporting it as required by law. This was a lie. Tiversa had no such concern.

61. When Boback learned that Mike Daugherty at LabMD ultimately refused to do business with Tiversa, Boback said to one of Tiversa's analysts, "f--- him, make sure he's at the top of the list." The "list" was a spreadsheet of companies Tiversa would soon give to the FTC.

Tiversa's Lies to CIGNA

62. One of the insurance companies listed in the 1718 file was CIGNA Health Insurance ("CIGNA"). In 2008, CIGNA was a Tiversa customer.

63. In April 2008, Tiversa sent an incident report to CIGNA stating that it had found a file on a peer-to-peer network with Personal Information on CIGNA insureds. Tiversa stated, "[a]fter reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that LabMD near Atlanta, Georgia is the disclosing source." This was *not* a lie.

64. In a report dated August 12, 2008, however, Tiversa told CIGNA, "The [1718 File], as well as some of the files not related to CIGNA, have been observed by Tiversa at additional IP addresses on the P2P." This was a lie.

65. Tiversa also told CIGNA in the August 12, 2008 report that (1) it had found the 1718 File in San Diego, CA at IP address 68.8.250.203 (designated "Proliferation Point #2") and (2) "other files present at Proliferation Point #2 suggest that this source could be an Information Concentrator." These were lies.

The FTC Strengthens its Alliance with Tiversa

66. Communications between Tiversa and the FTC continued through the winter and spring of 2009. Settlemyer introduced Sheer to Boback on or about March 4, 2009.

67. On information and belief, Settlemyer or Sheer (or both) introduced Yodaiken to Boback and others at Tiversa in the spring of 2009.

68. Sheer, Yodaiken and Settlemyer knew about the 1718 File in the spring of 2009.

69. Sheer, Yodaiken and Settlemyer knew or should have learned in the spring of 2009 that the filename of the 1718 file was "insuranceaging_6.05.071.pdf".

70. Sheer, Yodaiken and Settlemyer learned or should have learned in the spring of 2009 that the disclosing source of the 1718 File was an IP address for LabMD in Atlanta, Georgia.

71. Sheer, Yodaiken and Settlemyer learned or should have learned in the spring of 2009 that the *only* source of the 1718 File was an IP address for LabMD in Atlanta, Georgia.

72. Sheer, Yodaiken and Settlemyer learned or should have learned in the spring of 2009 that the 1718 File had not proliferated or spread anywhere on any peer-to-peer network.

The List

73. By the spring of 2009, Tiversa had developed a spreadsheet of approximately 100 companies that, according to Tiversa, had exposed Personal Information (the "List"). The companies on the List were companies to which Tiversa had tried but failed to sell Tiversa's remediation services. Tiversa scrubbed the List of the names of all existing or prospective Tiversa customers. As dictated by Boback, LabMD was included and placed near the top of the List.

74. Tiversa would later claim that it included several of its own customers on the List. This was a lie.

FTC Procedures and Rules of Practice

75. The behavior of FTC employees is mandated by the FTC's Procedures and Rules of Practice ("PRP") – the official rules of the agency.

76. "Commission investigations" under the PRP are inquiries conducted by a "Commission investigator" for the purpose of ascertaining whether any person is or has been engaged in any unfair or deceptive acts or practices in or affecting commerce or in any antitrust violations.

77. Under the PRP, the term "Commission investigator" means any attorney or investigator employed by the Commission who is charged with the duty of enforcing or carrying into effect any provisions relating to unfair or deceptive acts or practices in or affecting commerce or any provisions relating to antitrust violations.

78. At all times relevant to this Complaint, Defendants Sheer, Yodaiken and Settlemyer were Commission investigators.

79. The PRP authorizes the FTC to utilize civil investigative demands ("CIDs") in certain limited circumstances. The FTC does not have the authority to issue CIDs in the absence of an investigation.

80. The PRP mandates that each CID shall state the nature of the conduct constituting the alleged violation that is under investigation and the provision of law applicable to such violation.

81. Under the PRP, the production of documentary material in response to CIDs "shall be made under a sworn certificate, in such form as the demand designates, by the person, if a natural person, to whom the demand is directed or, if not a natural person, by any person having knowledge of the facts and circumstances relating to such production, to the effect that all of the documentary material required by the demand and in the possession, custody, or control of the person to whom the demand is directed has been produced and made available to the custodian."

The Privacy Institute

82. In the spring and summer of 2009, Sheer, Yodaiken and Settlemyer came to learn or should have come to learn that Boback and others at Tiversa were not honest or trustworthy. Sheer, Yodaiken and Settlemyer knew or had reason to know that Tiversa's internal documents

would prove that Boback and others at Tiversa could not be trusted and further knew or had reason to know that Tiversa's internal documents were likely to disprove allegations Tiversa would make about the source and spread of documents it "found" on peer-to-peer networks. Sheer, Yodaiken and Settlemyer also knew or had reason to know that Tiversa analysts would alter information in the Data Store to make it appear that Tiversa had located and downloaded files from the IP addresses of known identity thieves and further knew or had reason to believe that Tiversa analysts would create information in the Data Store as evidence of spread where, in fact, no spread had ever occurred.

83. Sheer, Yodaiken and Settlemyer knew or had reason to know that it would be extremely difficult, if not impossible, for companies the FTC investigated and prosecuted to disprove Tiversa's "evidence" of source and spread, unless those companies had access to Tiversa's internal documents.

84. Neither Sheer, Yodaiken, Settlemyer nor Boback wanted Tiversa to produce to the FTC any internal documents that would disprove Tiversa's evidence of source and spread. Specifically, Sheer, Yodaiken, Settlemyer and Boback did not want the FTC to use a compulsory process to obligate Tiversa to produce anything. To keep Tiversa from being legally obligated to produce *any* documents and to give Boback and Tiversa the freedom to produce whatever they wanted to the FTC, Sheer, Yodaiken, Settlemyer, Boback and others at Tiversa agreed that (1) Boback and Tiversa would create a shell company, (2) the FTC would issue a CID to the shell company instead of Tiversa, (3) Boback and Tiversa would "give" the shell company documents of their choosing, including a limited number of documents that supposedly contained incriminating evidence on future targets of FTC investigations and enforcement actions and (4) Boback and Tiversa could withhold from production whatever they wanted.

85. The shell company, created on June 3, 2009, was named "The Privacy Institute."

86. The Privacy Institute had no assets or employees. It was not legally related to Tiversa. Tiversa had no legal obligation to provide anything to The Privacy Institute and The Privacy Institute had no legal requirement to obtain anything from Tiversa.

87. By law, Sheer, Yodaiken and Settlemyer needed an FTC Commissioner to approve and sign the CID that would be served on The Privacy Institute on or about July 10, 2009.

88. By law, the CID could only issue in connection with an FTC investigation.

89. Tiversa was never the target of an FTC investigation or enforcement action.

90. The Privacy Institute was never the target of an FTC investigation or enforcement action.

91. Sheer and Yodaiken knew that the FTC was not authorized to issue CIDs with nothing more than a blanket request and knew that no FTC Commissioner was likely to sign such a CID. To induce an FTC Commissioner to sign and authorize a CID to be served on The Privacy Institute (the "PI CID"), Sheer and Yodaiken included in the proposed PI CID requests related to two companies already under investigation by the FTC – Rite-Aid and Walgreens. Sheer and Yodaiken also included a blanket request written to capture information on companies like LabMD that were *not* under investigation by the FTC. Sheer and Yodaiken knew this was improper, if not illegal, and knew that The Privacy Institute was just a façade. Sheer and Yodaiken were not concerned about the consequences of these actions because they knew that neither Tiversa nor The Privacy Institute would ever complain.

92. The FTC Commissioner who authorized and signed the PI CID would not have done so had he been told that Sheer and Yodaiken had plans to investigate parties other than

Rite-Aid and Walgreens that, like LabMD, had (1) already resolved any disclosure issues, (2) de minimus disclosures, (3) no disclosures, (4) no complaining witness, and (5) no originating source other than the company that would become the target of Sheer and Yodaiken's investigations.

93. Sheer, Yodaiken and Settlemyer knew that The Privacy Institute had no assets, no employees, no physical location and no documents or files. The Federal Defendants nevertheless served the PI CID on The Privacy Institute on or about July 10, 2009. Because The Privacy Institute had no documents, files or employees, the PI CID had no force of law. As a result, neither Tiversa nor The Privacy Institute had any obligation to produce *anything* to the FTC. Instead, Tiversa was free to provide whatever it wanted to the FTC.

94. In the fall of 2009, Boback and a Tiversa forensic analyst name Richard E. Wallace met in Washington, D.C. with Sheer, Yodaiken and/or other members of the FTC staff to discuss Tiversa's response to the CID served on The Privacy Institute. On information and belief, the FTC Staff expressed concerns that it did not have enough evidence to investigate companies where the only disclosing source was the company the FTC wanted to pursue.

95. On the return trip from Boback and Wallace's meeting with the FTC, Boback told Wallace that Tiversa needed to increase the apparent "spread" of the files identified on the List. Wallace was to search for the files again to see if they were available at IP addresses in addition to the address in the Data Store, and that if the files were not, in fact, available at any additional IP addresses, Wallace was told to create or alter data in the Data Store to make it appear that the files were available at additional IP addresses.

96. On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would provide whatever evidence

the FTC needed in its investigation and enforcement of companies on the List, even if the evidence was fraudulent. In so doing, Sheer, Yodaiken and Settlemyer conspired to deprive LabMD and Daugherty of their constitutional rights. LabMD and Daugherty were deprived of their constitutional rights as a result of this conspiracy.

97. On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would provide the FTC false evidence of source and spread. In so doing, Sheer, Yodaiken and Settlemyer conspired to deprive LabMD and Daugherty of their constitutional rights. LabMD and Daugherty were deprived of their constitutional rights as a result of this conspiracy.

98. On information and belief, Sheer, Yodaiken and Settlemyer knew or should have known in 2009 and thereafter that Boback and Tiversa would, upon request for additional evidence, manufacture and provide false evidence of source and spread. Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to allow this to happen and thereby deprived LabMD and Daugherty of their constitutional rights.

99. On information and belief, Sheer, Yodaiken and Settlemyer knew or should have known in 2009 and thereafter that Boback and others at Tiversa had and would provide false sworn testimony concerning source and spread. Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to allow this to happen and thereby deprived LabMD and Daugherty of their constitutional rights.

100. On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would withhold from production to the FTC and third parties documents and things that were exculpatory to LabMD and Daugherty.

Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to allow this to happen and thereby deprived LabMD and Daugherty of their constitutional rights.

101. On information and belief, Sheer, Yodaiken, Settlemyer, Boback and Tiversa expressly or tacitly agreed and conspired in 2009 to hurt, if not destroy, LabMD and to deprive Daugherty of his livelihood and property. Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to make this happen and thereby deprived LabMD and Daugherty of their constitutional rights.

102. Boback wanted revenge. Sheer, Yodaiken and Settlemyer wanted to make an example of LabMD. They believed, or should have known, that LabMD did not have the resources to sustain the kind of investigation they had in store for LabMD and Daugherty.

103. On July 27, 2009, Boback testified to the Oversight Committee on the topic of inadvertent file sharing for a second time. Boback testified that in February of that year, "Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One [the President's helicopter]. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran." This was a lie. Tiversa never found any files relating to Marine One on a computer with an IP address in Iran. On information and belief, Sheer, Yodaiken and Settlemyer knew this was a lie yet failed and refused to disclose their knowledge to responsible individuals at the FTC or other law enforcement agencies.

104. In August 2009, Tiversa, under the guise of The Privacy Institute, gave the List to the FTC. Tiversa also produced a screen shot showing that the disclosing source for the 1718 File was a computer with an IP address for LabMD in Atlanta, GA. Daugherty and LabMD would not know about this document or Sheer and Yodaiken's knowledge of it until years later.

Sheer and Yodaiken should have but refused to produce this document to Daugherty or LabMD at anytime during their investigation of Daugherty and LabMD.

105. Neither Tiversa nor The Privacy Institute ever provided any evidence that the 1718 File had proliferated on a peer-to-peer network. Sheer, Yodaiken and Settlemyer knew this but, on information and belief, consciously disregarded and failed to disclose these facts to responsible individuals at the FTC.

106. Daugherty and LabMD would not learn anything about The Privacy Institute before Boback's deposition on November 21, 2013. Until that point in time, neither Daugherty nor LabMD knew or had reason to know that Sheer, Yodaiken and Settlemyer, in their individual capacities:

- were acting outside the scope of their employment;
- were acting *ultra vires*;
- had deceived their superiors and others at the Commission;
- knew that Boback and Tiversa had committed crimes;
- were conspiring with Boback and Tiversa to create fraudulent incriminating evidence against LabMD and Daugherty;
- were conspiring with Boback and Tiversa to withhold evidence exculpatory to LabMD and Daugherty;
- were withholding evidence exculpatory to them; and
- were explicitly or implicitly conspiring to deprive Plaintiffs of their constitutional rights.

The FTC Gives Confidential Information to Boback

107. At some point before October 6, 2009, Sheer and/or Yodaiken violated FTC rules, policies, procedures and/or FTC guidance by disclosing to Boback intimate details about the FTC's upcoming investigations of the 100 or so companies on the List.

108. In October 2009, Boback bragged to employees of LifeLock about having inside knowledge from the FTC. Specifically, Boback told LifeLock on October 26, "the FTC is preparing the federal cases against 100 or so companies that have breached consumers information via P2P." On October 6, Boback told LifeLock, "The FTC letters did not go out yet so the companies will not know what you will be talking about...yet."

109. Boback further explained to LifeLock that the Washington Post planned to "shame" companies into addressing the problem, and that the upcoming FTC investigations presented a unique opportunity for LifeLock and Tiversa to profit.

110. On October 20, 2009, a Tiversa analyst e-mailed Boback the name, resume, and Facebook profile picture of a House Ethics Committee staffer who would become part of a story published by the Washington Post nine (9) days later. Boback thereafter told LifeLock "…there was a breach in House Ethics via 2P2 that the Washington Post will be writing a story about this week or next…." Boback knew this because Boback gave the information to the Washington Post.

111. On information and belief, Boback bragged to Sheer, Yodaiken and Settlemyer about he and Tiversa being the undisclosed sources for the Washington Post story.

112. Boback thereafter tried to get the House Ethics Committee to hire Tiversa by showing the "spread" on the leak.

113. From August 2009 through January 2010, Tiversa employees called Defendant Sheer at least 34 times.

114. On December 22, 2009, the White House announced that President Obama appointed Howard Schmidt to be the President's new White House Cybersecurity Coordinator. On information and belief, Schmidt was still a member of Tiversa's Advisory Board at the time of his appointment. On information and belief, Schmidt had an equity interest in Tiversa at the time of his appointment. On information and belief, Schmidt kept his equity interest in Tiversa during his service as White House Cybersecurity Coordinator. On information and belief, at Boback's behest, Schmidt influenced the FTC in general and Sheer in particular, to vigorously pursue an investigation and enforcement action against LabMD, regardless of the merits of the pursuit. On information and belief, Sheer told or otherwise indicated to Schmidt that he would.

115. Soon after the announcement of Schmidt's appointment, Daugherty received a letter dated January 19, 2010, from Sheer informing LabMD that the FTC was "conducting a non-public inquiry into LabMD's compliance with federal law governing information security." The letter states, "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"). This was a lie. Sheer knew that neither the 1718 File nor any other LabMD file was available to anyone on any peer-to-peer network. On information and belief, Sheer knew from conversations with Boback and others that when Tiversa contacted LabMD in May 2008, LabMD immediately found and removed the offending software (LimeWire) and that, thereafter, there was no basis for an inquiry or investigation of any sort.

116. The FTC's investigation of LabMD and Daugherty (the "Investigation") continued for three and a half years. It was an intrusive and exhaustive, multiyear civil

investigation in which Sheer and Yodaiken issued burdensome voluntary access requests and civil investigative demands to LabMD, obtained thousands of pages of documents from LabMD and Daugherty, and deposed, under oath, LabMD principals, causing LabMD's insurance carriers to cancel LabMD's insurance coverage and causing crippling economic hardship and reputational harm.

117. LabMD and Daugherty produced thousands of pages of documents, sat for hours of interviews and met with the FTC on numerous occasions by telephone and in person, only to be told by Sheer and Yodaiken, time after time, that LabMD's responses were inadequate.

118. At no time during the Investigation did Sheer, Yodaiken or Settlemyer disclose to LabMD the evidence the FTC received from The Privacy Institute establishing that LabMD was the *only* source of the 1718 File. Nor did they disclose their knowledge that Tiversa obtained the 1718 file by hacking into LabMD's computer network.

119. At no time during the Investigation did Sheer, Yodaiken or Settlemyer inform LabMD that the FTC had received documents from Tiversa via The Privacy Institute, a sham organization.

120. At no time during the Investigation did Sheer or Yodaiken issue a CID to Tiversa for documents and information relating to the 1718 File.

121. Not a single patient has ever been harmed by the alleged disclosures of the 1718 file.

122. On August 31, 2011, the FTC demanded that Daugherty and LabMD sign consent decrees admitting to an unfair trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, due to inadequate data security practices. LabMD and Daugherty refused to

sign the consent decrees, making their positions clear to Sheer and Yodaiken on October 20, 2011.

123. In retaliation for Daugherty and LabMD's refusals to sign consent decrees, the FTC issued CIDs to LabMD and Daugherty on December 21, 2011. In response, LabMD and Daugherty moved the FTC Commissioners to quash the CID on the ground that the FTC lacked authority to issue the CID, especially because the FTC was relying upon evidence from Tiversa, a private party with a commercial interest. All but one of the FTC Commissioners denied the motion to quash. FTC Commissioner J. Thomas Rosch said in his dissent, "I do not agree that [FTC] staff should further inquire - either by document request, interrogatory, or investigational hearing - about the 1,718 File." Commissioner Rosch explained the reason for his dissent:

> Specifically, I am concerned that Tiversa is more than an ordinary witness, informant, or "whistle-blower." It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. In my view, while there appears to be nothing per se unlawful about this evidence, the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

124. On information and belief, Sheer and Yodaiken misrepresented material facts to the Commission, failed to disclose material facts to the Commission and thereby caused the majority of the Commissioners to deny LabMD and Daugherty's motion to quash. On information and belief, Sheer and Yodaiken expressly or impliedly agreed to deprive LabMD and Daugherty of their constitutional rights by intentionally misrepresenting facts and omitting to inform their superiors and the Commissioners as follows:

- The FTC's primary "evidence" against LabMD was a file taken by Tiversa when Tiversa hacked directly into a LabMD computer;

- The only way for a user to locate the 1718 File on a peer-to-peer network was to have used the highly unusual search terms "insuranceaging" or "6.05.071";
- By accessing, downloading and retaining the 1718 File, Tiversa violated several federal and state crimes;
- The LabMD computer hacked by Tiversa was the *only* source of the 1718 File;
- When Tiversa notified LabMD it had a copy of the 1718 File, LabMD started an immediate investigation and, within minutes of its discovery of an unauthorized installation of LimeWire on one of its billing computers, removed the offending software;
- Boback and Tiversa were unreliable and not credible;
- Boback and Tiversa had manufactured evidence to make it appear that the 1718 File and files of other companies had proliferated on peer-to-peer networks when, in fact, they had not;
- Sheer, Yodaiken and Boback agreed to create a sham company to receive a CID from the FTC and that Tiversa, the actual custodian of the requested documents, was free to withhold from and provide to the FTC whatever evidence it wanted;
- There were no complaining witnesses; and
- Not one single patient suffered harm due to any alleged disclosure of the 1718 file.

125. As a result of Sheer and Yodaiken's omissions and misrepresentations to the FTC Commissioners, LabMD and Daugherty were deprived of their constitutional rights.

126. LabMD and Daugherty fought but ultimately complied with the CIDs, endured two more civil investigative hearings and produced yet more documents to Sheer and Yodaiken.

127. After years of FTC pressure and intimidation, Daugherty began speaking out regarding LabMD's ordeal with the FTC. Daugherty leveled sharp criticisms at the conduct of

the FTC in general and Sheer and Yodaiken in particular. Specifically, in early 2012, Mr. Daugherty began to warn the public about the FTC's abuses (orchestrated by Sheer and Yodaiken) through the press and social media and through a book, all to express his outrage at the way that LabMD was being treated by the federal government. Mr. Daugherty used, and continues to use, the website, http://michaeljdaugherty.com/, to criticize the government.

128. Daugherty was quoted in the September 7, 2012 edition of the Atlanta Business Chronicle saying: "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." The reporter wrote in her story that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about $500,000 fighting the investigation."

129. Three days later, on September 10, 2012, an FTC paralegal downloaded the Atlanta Business Chronicle article from LexisNexis and, on information and belief, disseminated it to Sheer, Yodaiken and other FTC staff members.

130. After reading Daugherty's quote, Sheer and Yodaiken ramped up their investigative efforts against Daugherty and LabMD.

131. On July 19, 2013, Daugherty posted a trailer on the internet for *The Devil Inside the Beltway*, a book he had written about his dealings with Sheer, Yodaiken and others at FTC. The trailer referred to the FTC's actions as 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." The trailer was especially critical of Sheer.

132. On July 22, 2013, just three days after the trailer for *The Devil Inside the Beltway* was posted on the internet, Sheer told a LabMD attorney that he and his staff recommended an enforcement action against LabMD.

The Enforcement Action

133. In their roles as Commission investigators, Defendants Sheer and Yodaiken convinced their superiors and, ultimately, the FTC Commissioners, to authorize an administrative enforcement action against LabMD. They did so by concealing the truth and misrepresenting the facts. The FTC Commissioners would not have authorized the Enforcement Action if Sheer and Yodaiken had been truthful and forthcoming with the facts. On information and belief, Sheer and Yodaiken expressly or impliedly agreed to deprive LabMD and Daugherty of their constitutional rights by intentionally misrepresenting facts and omitting to inform their superiors and the Commissioners as follows:

- The FTC's primary "evidence" against LabMD was a file taken by Tiversa when Tiversa hacked directly into a LabMD computer;
- The only way for a user to locate the 1718 File on a peer-to-peer network was to have used the highly unusual search terms "insuranceaging" or "6.05.071";
- By accessing, downloading and retaining the 1718 File, Tiversa violated several federal and state crimes;
- The LabMD computer hacked by Tiversa was the *only* source of the 1718 File;
- When Tiversa notified LabMD it had a copy of the 1718 File, LabMD started an immediate investigation and, within minutes of its discovery of an unauthorized installation of LimeWire on one of its billing computers, removed the offending software;

- Boback and Tiversa were unreliable and not credible;
- Boback and Tiversa had manufactured evidence to make it appear that the 1718 File and files of other companies had proliferated on peer-to-peer networks when, in fact, they had not;
- Sheer, Yodaiken and Boback agreed to create a sham company to receive a CID from the FTC and that Tiversa, the actual custodian of the requested documents, was free to withhold from and provide to the FTC whatever evidence it wanted;
- There were no complaining witnesses; and
- Not one single patient suffered harm due to any alleged disclosure of the 1718 file.

134. On August 28, 2013, the FTC Commissioners, relying upon Sheer and Yodaiken's misrepresentations and omissions, voted unanimously (4-0) to issue an administrative enforcement action Complaint against LabMD because LabMD had supposedly failed to provide "reasonable and appropriate security" for patient information and that this was an "unfair" act or practice in violation of Section 5.

135. The FTC filed the administrative enforcement action against LabMD on August 28, 2013 (the "Enforcement Action"). The FTC alleged that LabMD's data security practices violated unspecified standards and were "unfair" acts or practices in violation of Section 5. That same day, the FTC issued a press release and posted a blog celebrating their actions and harshly criticizing LabMD, thereby harming LabMD's public reputation.

136. Sheer was lead counsel in the Enforcement Action until the fall of 2014 when he was interviewed by the Oversight Committee in the Committee's investigation of the relationship between the FTC and Tiversa and the veracity of the information provided by Tiversa to Sheer and Yodaiken.

137. On August 29, 2013, several weeks before *The Devil Inside the Beltway* was published, the FTC issued a press release harshly criticizing LabMD. That same day, the FTC also published a "blog post" about their actions in which they made disparaging claims about LabMD and ominously framed the LabMD Complaint as a warning to other businesses: "If your clients are focused on data security —and they should be—here's a development they'll want to know about." Lesley Fair, "FTC Files Data Security Complaint Against LabMD," Business Center Blog (Aug. 29, 2013).

138. *The Devil Inside the Beltway* was published on September 24, 2013.

139. On September 30, 2013, the FTC served a subpoena on Tiversa. Tiversa failed to fully respond to the subpoena. Among other categories of documents, the subpoena requested "all documents related to LabMD." In its response, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the 1718 File. In total, Tiversa produced 8,669 pages of documents in response to the subpoena. Because the production contained *five* copies of the 1718 File, only 79 pages of other documents remained.

140. Sheer knew that Tiversa's response to the subpoena was inadequate but took no action to compel Tiversa to fully comply with the subpoena. Sheer's purpose for serving the Tiversa subpoena was to give the appearance of independence, not to obtain evidence. In truth, Sheer had no desire to uncover any additional evidence from Tiversa, especially if the evidence was exculpatory for Daugherty and LabMD.

141. The FTC did not subpoena The Privacy Institute. That entity dissolved on or about June 18, 2013, approximately two months before the Enforcement Action began.

142. October 24, 2013, Sheer retaliated against LabMD and Daugherty by serving a subpoena on Daugherty requesting the following documents concerning Daugherty's book:

- "All drafts of … [LabMD's CEO's book about the Defendants] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" LabMD's CEO's book about the Defendants.
- "All documents related to the source material for drafts of" LabMD's CEO's book about the Defendants, "including documents referenced or quoted in the" book. (Complaint Counsel has defined "related" broadly 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.")
- "All promotional materials related to" LabMD's CEO's book criticizing Defendants, "including, but not limited to, documents posted on social media, commercials featuring … [LabMD's CEO], and presentations or interviews given by" LabMD's CEO.

143. To punish LabMD, Sheer filed or caused to be filed burdensome, duplicative, and oppressive discovery requests that would not be allowed by an independent Article III court.

144. Sheer caused the FTC to serve LabMD's customers and other third parties, almost none of whom had anything to do with the matters at issue in the Enforcement Action, with wrongfully intrusive and burdensome subpoenas.

145. Upon information and belief, Sheer recommended the Enforcement Action to punish and to make an example of LabMD and Daugherty, both for refusing to sign consent orders and for exercising First Amendment rights to engage in constitutionally protected speech about a matter of public concern and criticize the government without fear of government reprisal.

146. One of the documents produced in the Enforcement Action by Sheer, CX0019, purports to show that Tiversa had downloaded the 1718 File from four IP addresses on particular dates and times. In truth, Tiversa analyst Wallace created CX0019, at Boback's direction, in 2013, near the time of Boback's deposition, to make it appear that the 1718 File had "spread" to IP addresses belonging to known identity thieves, and that the 1718 File had not been found at an Atlanta IP address. Boback specifically asked Wallace to include a San Diego IP address. These were lies and CX0019 was fraudulent. Sheer knew that CX0019 was fraudulent but proceeded with the evidence anyway.

147. In 2014, the Chairman of the Oversight Committee commenced an investigation of Tiversa regarding its involvement with government agencies. The investigation continued over a period of months and included investigation into Tiversa's relationship with the FTC.

148. The Oversight Committee staff report regarding its 2014 investigation concluded, inter alia, that Tiversa and Boback provided incomplete, inconsistent, and/or conflicting information to the FTC in this matter.

149. In the fall of 2014, after being interviewed by the Oversight Committee, Sheer was removed from the role of lead counsel in the Enforcement Action.

The Initial Decision

150. On November 13, 2015, Chief Administrative Law Judge D. Michael Chappell issued an Initial Decision wherein he concluded that the FTC had failed to carry its burden of proving its theory that LabMD's alleged failure to employ reasonable data security constitutes an unfair trade practice because Complaint Counsel has failed to prove the first prong of the three-part test – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.

151. Judge Chappell made the following findings and conclusions:

- With respect to the 1718 File, the FTC's evidence failed to prove that the limited exposure of the 1718 File has resulted, or is likely to result, in any identity theft-related harm.
- With respect to the exposure of certain LabMD "day sheets" and check copies, the FTC failed to prove that the exposure of these documents is causally connected to any failure of LabMD to reasonably protect data maintained on its computer network, as alleged in the Complaint, because the evidence fails to show that these documents were maintained on, or taken from, LabMD's computer network. In addition, the FTC failed to prove that this exposure has caused, or is likely to cause, any consumer harm.
- Judge Chappell rejected the FTC's argument that identity theft-related harm is likely for all consumers whose personal information is maintained on LabMD's computer networks, even if their information has been not exposed in a data breach, on the theory that LabMD's computer networks are "at risk" of a future data breach.
- Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case.
- Unjustified consumer injury is the primary focus of the FTC Act.
- The Commission has stated that its "concerns should be with substantial consumer injuries; its resources should not be used for trivial or speculative harm."
- The preponderance of the evidence in this case failed to show that LabMD's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury.

Accordingly, the Complaint must be dismissed, and it need not, and will not, be further determined whether or not LabMD's data security was, in fact, "unreasonable."

- Unfair conduct cases usually involve actual and completed harms.
- Historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm.
- The record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged failure to employ "reasonable" data security for its computer networks, including in connection with the Security Incidents alleged in the Complaint.
- The FTC did not identify even one consumer that suffered any harm as a result of LabMD's alleged unreasonable data security.
- Given that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.
- Strangely, the FTC took no position as to how the Sacramento Documents came into the possession of the individuals in Sacramento, and further admits that "there is no conclusive explanation of how LabMD Day Sheets were exposed."
- The evidence shows that the 1718 File was available for peer-to-peer sharing through LabMD no earlier than June 2007 (the date of the document) until May 2008, when LabMD removed LimeWire from the billing computer.
- Although the 1718 File was available for downloading during this period, the evidence fails to show that the 1718 File was in fact downloaded by anyone other than Tiversa, who obtained the document in February 2008.

- Because of Boback's biased motive, Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of LabMD.
- Boback was evasive and lacked forthrightness in response to questioning during his June 7, 2014 video deposition taken by LabMD for purposes of trial testimony.
- Boback's testimony in this case is not credible.
- Boback's 2013 discovery deposition, Boback's 2014 trial deposition testimony, and a Tiversa-provided exhibit, CX0019, are unreliable, not credible, and outweighed by credible contrary testimony from Wallace.
- Tiversa's Data Store is not a credible or reliable source of information as to the disclosure source or the spread of any file purportedly found by Tiversa.
- Former Commissioner Rosch advised in April 2012, in his dissenting opinion on LabMD's Motion to Quash or Limit Civil Investigative Demand, that, under these circumstances, the FTC staff should not inquire about the 1718 File, and should not rely on Tiversa for evidence or information, in order to avoid the appearance of impropriety. Judge Chappell noted FTC staff did not heed then-Commissioner Rosch's warning, and also did not follow his advice. Instead, Complaint Counsel chose to further commit to and increase its reliance on Tiversa.

152. Sheer, Yodaiken, Settlemyer, Boback and Tiversa have won. Through the Federal Defendants' abuses of power and disregard for the core constitutional rights of LabMD and Daugherty, the Federal Defendants have put LabMD out of business and laid it to rest. In addition, they have deprived Daugherty of his right to make a living from an extremely valuable asset that he built from the ground up.

CLAIMS FOR RELIEF

COUNT I
(Constitutional Violation – First Amendment, Freedom of Speech)
(All Defendants)

153. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 152 above, as if fully set forth verbatim in this Count I.

154. Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to express their information, thoughts, opinions, beliefs, ideas and creativity and other protections and violated Plaintiffs' other rights and privileges in the First Amendment.

155. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT II
(Constitutional Violation – First Amendment, Freedom of the Press)
(All Defendants)

156. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 155 above, as if fully set forth verbatim in this Count II.

157. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to publish their information, thoughts, opinions, beliefs, ideas and creativity and violated Plaintiffs' other rights and privileges in the First Amendment.

158. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT III
(Constitutional Violation – First Amendment, Right to Petition Government for Redress of Grievances)
(All Defendants)

159. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 158 above, as if fully set forth verbatim in this Count III.

160. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to petition their government and elected officials for redress of their concerns and grievances and violated Plaintiffs' other rights and privileges in the First Amendment.

161. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT IV
(Constitutional Violation – Fourth Amendment, Unreasonable Search and Seizure)
(All Defendants)

162. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 161 above, as if fully set forth verbatim in this Count IV.

163. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights against unlawful search and seizure and violated Plaintiffs' other rights and privileges in the Fourth Amendment.

164. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT V
(Constitutional Violation – Fifth Amendment, Procedural Due Process)
(All Defendants)

165. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 164 above, as if fully set forth verbatim in this Count V.

166. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to procedural due process and violated Plaintiffs' other rights and privileges in the Fifth Amendment.

167. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT VI
(Constitutional Violation – Fifth Amendment, Substantive Due Process)
(All Defendants)

168. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 167 above, as if fully set forth verbatim in this Count VI.

169. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to substantive due process and violated Plaintiffs' other rights and privileges in the Fifth Amendment.

170. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT VII
(Civil Conspiracy under Federal Common Law)
(All Defendants)

171. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 170 above, as if fully set forth verbatim in this Count VII.

172. The Federal Defendants expressly and impliedly agreed among themselves to deprive Plaintiffs of their constitutions rights.

173. The Federal Defendants actually deprived Plaintiffs of their constitutional rights as a result of their express and implied agreements.

PRAYER FOR RELIEF

WHEREFORE, Daugherty and LabMD respectfully demands the following relief:

a) That Daugherty and LabMD recover from and have judgment against Federal Defendants, sued in their individual capacities, jointly and severally, in such sums as sufficient to fully compensate Plaintiffs for all of their damages, losses and injuries sustained as a result of the facts set forth above, including, without limitation, consequential, general, nominal and special damages as well as punitive damages in amounts to be determined by the enlightened conscience of the jury;

b) For an award of reasonable attorneys' fees and costs against Federal Defendants; and

c) For such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs seek a trial by jury of all issues so triable.

Dated: November 20, 2015

Respectfully submitted,

/s/Jason H. Ehrenberg

Jason H. Ehrenberg (#469077)
Peter K. Tompa (#413752)
BAILEY & EHRENBERG PLLC
1015 18th Street, NW
Suite 204
Washington, DC 20036
Phone: 202.331.4209
Facsimile: 202.318.7071
jhe@becounsel.com

and

James W. Hawkins
Pro hac vice (application to be filed)
Georgia State Bar No. 338767
JAMES W. HAWKINS, LLC
11339 Musette Circle
Alpharetta, GA 30009
V: 678-697-1278
F: 678-540-4515
jhawkins@jameswhawkinsllc.com

Attorneys for Plaintiffs Michael J. Daugherty and LabMD, Inc.

EXHIBIT B

ORIGINAL

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

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

ORDER ON COMPLAINT COUNSEL'S MOTION TO QUASH SUBPOENA SERVED ON COMPLAINT COUNSEL AND FOR PROTECTIVE ORDER

On January 6, 2014, Complaint Counsel filed a Motion to Quash Subpoena Served on Complaint Counsel and for a Protective Order ("Motion"). Complaint Counsel seeks an order quashing a subpoena *ad testificandum* served by Respondent LabMD ("Respondent" or "LabMD") on Senior Complaint Counsel Alain Sheer and barring Respondent in the future from serving any subpoena *ad testificandum* on any Complaint Counsel attorneys. Respondent filed its opposition on January 16, 2014 ("Opposition").

Having fully reviewed the Motion and the Opposition, and considered all arguments and contentions raised therein, the Motion is GRANTED IN PART AND DENIED IN PART, 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. Complaint ¶ 23. Specifically, the Complaint alleges that Respondent failed to maintain adequate network security to protect confidential patient information, including by making certain "insurance aging reports," allegedly containing confidential patient information, available on a peer-to-peer, or "P2P" file sharing application. Complaint ¶¶ 17, 19. The Complaint further avers that in October 2012, the Sacramento, California Police Department found more than 35 LabMD "day sheets," allegedly containing confidential patient information ("Day Sheets") [1], and a small number of copied checks in the possession of individuals who subsequently pleaded no contest to state charges of identity theft. Complaint ¶ 21.

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

Respondent's Answer admits that an alleged third party, Tiversa Holding Corporation ("Tiversa"), contacted Respondent in May 2008 and claimed to have obtained the P2P insurance aging file via Limewire, but denies that Respondent violated the FTC Act or that any consumer was injured by the alleged security breach. Answer ¶¶ 17-23. Respondent's answer also includes a number of affirmative defenses, including among others, failure to state a claim, lack of subject matter jurisdiction, denial of due process and fair notice, and that the actions of the FTC are arbitrary, capricious, an abuse of discretion, and otherwise not in accordance with applicable law. Answer at pp. 6-7.

Although Respondent's subpoena does not designate any topics for Mr. Sheer's deposition, according to Respondent's Opposition, Respondent seeks to inquire into the following areas:

1. Mr. Sheer's communications with the Sacramento Police Department ("SPD") in or around December 2012 regarding SPD's discovery of LabMD Day Sheets;

2. Mr. Sheer's communications with Tiversa in meetings and/or conference calls taking place in 2009;

3. Mr. Sheer's communications with Dartmouth College via email in March 2009, regarding a study that Dartmouth conducted on health information available on P2P networks and whether the FTC and Dartmouth "exchanged information" regarding LabMD's alleged data security breach; and

4. Mr. Sheer's knowledge regarding the FTC's "analys[e]s and processes including any rules, regulations, and guidelines, which led the FTC to its decision to investigate LabMD and other similarly situated victims of cyber theft as a means to expand its authority under section 5." Opposition at 3-4.

II. Overview of Applicable Law

The general scope of discovery is set forth in Commission Rule of Practice 3.31(c), which provides in pertinent part: "Parties may obtain discovery to the extent that it may be reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses of any respondent." 16 C.F.R. § 3.31(c)(1). However, a party may not seek discovery that is "unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive"; or where the burden or expense of providing the discovery outweighs its likely benefit. 16 C.F.R. § 3.31(c)(2)(i); *see also* 16 C.F.R. § 3.31(d) (Administrative Law Judge "may also deny discovery . . . to protect a party or other person from annoyance, embarrassment, oppression, or undue burden or expense, or to prevent undue delay in the proceeding.").

In light of the generally broad scope of permissible discovery, opposing trial counsel is not "absolutely immune from being deposed," *Shelton v. Am. Motors Corp.*, 805 F.2d 1323, 1327 (8th Cir. 1986), but such discovery is, nevertheless, generally disfavored. *Official Comm. of Unsecured Creditors of Hechinger Inv. Co. of Del., Inc. v. Friedman (In re*

Subpoena Issued to Dennis Friedman), 350 F.3d 65, 71-72 (2d Cir. 2003); *Nguyen v. Excel Corp.*, 197 F.3d 200, 208-09 (5th Cir. 1999); *Corporation v. American Auto. Centennial Comm'n*, 1999 U.S. Dist. LEXIS 1072, at * 3 (D.D.C. Feb. 2, 1999). "Most courts which have addressed [requests to depose opposing counsel] have held that the taking of opposing counsel's deposition should be permitted only in limited circumstances and that, because of the potential for abuse inherent in deposing an opponent's attorney, the party seeking the deposition must demonstrate its propriety and need before the deposition may go forward." *American Casualty Co. v. Krieger*, 160 F.R.D. 582, 588 (S.D. Cal. 1995). Accordingly, when, as here, a party seeks to depose opposing trial counsel, the party seeking such discovery must show: "(1) no other means exist to obtain the information than to depose opposing counsel, . . . ; (2) the information sought is relevant and nonprivileged; and (3) the information is crucial to the preparation of the case." *Shelton*, 805 F.2d at 1323; *Nationwide Mut. Ins. Co. v. Home Ins. Co.*, 278 F.3d 621, 628 (6th Cir. 2002); *see Friedman*, 350 F.3d at 71-72, and cases cited therein (hereafter, the "*Shelton* factors"). *See In re Hoechst Marion Roussel, Inc.*, 2000 WL 33944050, at *1 (Nov. 8, 2000) (applying *Shelton* factors to deny motion to compel depositions of, among others, FTC attorneys).

As the court stated in *American Casualty*:

> There are good reasons to require the party seeking to depose another party's attorney to bear the burden of establishing the propriety and need for the deposition. "While the Federal Rules do not prohibit the deposition of a party's attorney, experience teaches that countenancing unbridled depositions of attorneys constitutes an invitation to delay, disruption of the case, harassment, and perhaps disqualification of the attorney . . ."

160 F.R.D. at 588 (quoting in part *N.F.A. Corp. v. Riverview Narrow Fabrics, Inc.*, 117 F.R.D. 83, 85 (M.D.N.C. 1987)).

Based on the foregoing, the analysis now turns to whether Respondent has met its burden of demonstrating that the information that Respondent seeks to obtain can only be obtained from Mr. Sheer; that the information is both relevant and nonprivileged; and that the desired information is crucial to Respondent's case.

III. Analysis

A. Whether other means exist to obtain the information than to depose opposing counsel

Respondent argues that only Mr. Sheer can provide information regarding the FTC's communications with nonparties SPD, Tiversa, and Dartmouth College, and "the FTC's behavior . . ." regarding this case. Respondent sets forth, as an example of Mr. Sheer's allegedly unique knowledge, that only Mr. Sheer "can testify why the FTC waited four months to notify LabMD about the Day Sheets [found in Sacramento and provided to the FTC by SPD] and why the FTC never contacted the consumers" to advise them that their personal information may have been compromised. Opposition at 5. However, the testimony of Ms.

Jestes of the SPD, upon which Respondent relies, says nothing regarding whether or not the FTC notified LabMD about the Day Sheets. In addition, Ms. Jestes does not state that the FTC never contacted consumers, as Respondent asserts.[2] Accordingly, the factual premises underlying Respondent's argument are unsupported.

Respondent further asserts that only Mr. Sheer can testify as to the substance of communications with Tiversa because, according to Respondent, Mr. Bobak, CEO of Tiversa, "testified that he had conversations with Sheer, but could not remember the substance of them." Opposition at 5. This asserted example is also not supported by the record presented. According to the deposition excerpts provided by Respondent, Mr. Bobak testified that there were two meetings with FTC representatives in 2009. "One at Tiversa here in Pittsburgh. And one at the FTC in DC." Opposition Exh. 1 at 140. The pertinent testimony follows:

> Q: Do you recall who was in attendance at the meeting in Pittsburgh?
> A: I do. Alain Sheer and I believe it was a woman that was with him. But I don't know who she was.
> . . .
> Q: I'm sorry. Do you recall who was in attendance at [the DC meetings]?
> A: Alain Sheer, and I don't really recall. There were other people, maybe another person or two, but I don't specifically recall who they were.
> Q: At those meetings, was LabMD specifically discussed?
> A: In the meeting in Pittsburgh, no. In the meeting in DC it may have been, but only in the context of multiple organizations as well. . . . [T]here was no extended time on LabMD any more than any of the other organizations . . . .

Opposition Exh. 1 at 140-141.

Thus, while Mr. Bobak testified that he was unable to remember the names of all the FTC representatives with whom Tiversa met, Mr. Bobak clearly recalled that LabMD was not discussed at all at one of the two meetings involving Mr. Sheer, and that LabMD was discussed at the other meeting along with, and no more than, various other entities. Thus, contrary to Respondent's representation, according to the deposition excerpts provided by Respondent, Mr. Bobak did not testify that he could not remember the substance of his conversation(s) with Mr. Sheer. Indeed, the deposition record provided does not indicate that Mr. Bobak was asked any generalized questions about the substance of these conversations, but was asked only if LabMD was specifically discussed.

With regard to Mr. Sheer's asserted knowledge of the FTC's communications with Dartmouth College, Respondent has failed to demonstrate that it has sought to depose any representatives of Dartmouth, including the Dartmouth individual identified in the emails

[2] Indeed, Ms. Jestes' testimony, provided by Respondent, contradicts Respondent's assertion that the FTC never contacted consumers. *See* Opposition Exh. 4 at 72 (Q: To this day are you aware whether the FTC has notified any of the people identified on the LabMD documents with respect to the fact their protected personal information may have been inappropriately released? A: Yes. . . . I received a phone call from a gentleman that received the letter . . . . We had a conversation of [how] he received the letter and what should he do, and I referred him back to the . . . links" from the FTC web page provided by the FTC to Ms. Jestes.).

upon which Respondent relies to show communications between Mr. Sheer and Dartmouth. Accordingly, Respondent has failed to meet its burden of demonstrating that Mr. Sheer's deposition testimony is "the only means" by which Respondent can obtain information regarding communications with SPD, Tiversa, or Dartmouth College. Moreover, Respondent failed to provide any facts or argument to support a conclusion that only Mr. Sheer can provide information regarding the FTC's analyses and/or processes underlying the decision to investigate LabMD or the decision to apply the FTC's Section 5 "unfairness" authority to address LabMD's patient information security practices.[3] Thus, Respondent has failed to prove the first prong of the *Shelton* factors.

B. Whether the information sought is relevant and nonprivileged

The second prong that Respondent must establish is that the information sought is both relevant and nonprivileged. As set forth below, Respondent has not met its burden on this prong of the *Shelton* factors.

Respondent asserts, without further explanation, that testimony from Mr. Sheer is relevant to "certain essential elements of Complaint Counsel's case." Such conclusory, unsupported assertions do not demonstrate relevance. *See In re Intel Corp.*, Docket No. 9341, 2010 FTC LEXIS 48, at *4 (May 28, 2010) (denying motion to quash where assertions that proposed deponents had no relevant knowledge were unsupported "conclusory assertions"). Respondent also asserts that the testimony sought from Mr. Sheer goes directly to certain elements of Complaint Counsel's case and to LabMD's defenses that: (1) the "Complaint fails to state a claim upon which relief can be granted;" (2) "the Commission is without subject-matter jurisdiction over the claims asserted in this case;" (3) "the Commission's actions are arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;" (4) "the acts or practices alleged in the Complaint do not cause, and are not likely to cause, substantial injury to consumers that is not reasonably avoidable by consumers themselves;" and (5) "the enforcement in this action against LabMD violates the due process requirements of fair notice." Opposition at 6. Specifically, Respondent asserts, Respondent believes "that Sheer's testimony regarding his communications with Tiversa, Dartmouth, and the SPD will be helpful in determining whether the Commission's actions in investigating and filing a complaint against LabMD were arbitrary and capricious, an abuse of discretion, and in violation of due process." *Id.*

Complaint Counsel argues that testimony about the Commission's pre-complaint process and decision to issue a complaint against LabMD are not relevant or reasonably calculated to lead to the discovery of admissible evidence. Motion at 5-6.

In *In re Exxon Corp.*, Docket No. 8934, 83 F.T.C. 1759, 1974 FTC LEXIS 226 (June 4, 1974), the Commission held:

[3] Respondent does not dispute Complaint Counsel's assertion that the only discovery Respondent has conducted in this case so far consists of document subpoenas issued to Tiversa and SPD; deposition subpoenas issued to Tiversa and Complaint Counsel; and interrogatories and document requests issued to Complaint Counsel.

> [I]t has long been settled that the adequacy of the Commission's "reason to believe" a violation of law has occurred and its belief that a proceeding to stop it would be in the "public interest" are matters that go to the mental processes of the Commissioners and will not be reviewed by the courts. Once the Commission has resolved these questions and issued a complaint, the issue to be litigated is not the adequacy of the Commission's pre-complaint information or the diligence of its study of the material in question but whether the alleged violation has in fact occurred.

Id. at *2-3. *See also In re Exxon Corp.*, Docket 8934, 1981 FTC LEXIS 113, at *5-6 (Jan. 29, 1981) (quoting *Exxon*, 83 F.T.C. at 1760 and denying on relevance grounds respondent's renewed request for discovery into whether the Commission had "reason to believe" that a violation of law had occurred). "Once a complaint issues, 'only in the most extraordinary circumstances' will the Commission review its reason to believe and public interest determinations." *In re Boise Cascade Corp.*, 97 F.T.C. 246, 1981 FTC LEXIS 71, at *3 n.3 (March 27, 1981) (citing *TRW Inc.*, 88 F.T.C. 544 (1976)). Respondent has made no showing that any such extraordinary circumstances are present here.

Similarly, in *In re Basic Research*, 2004 FTC LEXIS 210, *10-11 (Nov. 4, 2004), respondent's motion to compel a response to an interrogatory seeking information regarding why the complaint was not filed prior to June 2004 was denied on the basis that such information was not relevant to any pending issues in the case. The ALJ stated, "the issue to be tried is whether Respondent disseminated false and misleading advertising, not the Commission's decision to file the Complaint." *Id.* (citing *Boise Cascade Corp. v. FTC*, 498 F. Supp. 772 (D. Del. 1980); *In re Exxon Corp.*, 1981 FTC LEXIS 113 (Jan. 19, 1981)). *See also In re Hoechst Marion Roussel, Inc.*, 2000 WL 33944050, at *1 (Nov. 8, 2000) (denying respondent's motion to compel depositions of certain FTC attorneys and others concerning pre-complaint discussions that they had with the respondent).

It is beyond dispute that Respondent's purpose in eliciting information concerning the pre-Complaint investigation and the Commission's decision making in issuing the Complaint is to challenge the bases for the Commission's commencement of this action. Precedent dictates that such matters are not relevant for purposes of discovery in an administrative adjudication. Moreover, Respondent fails to cite any Commission case where discovery of such matters was permitted, much less through questioning of trial counsel. Accordingly, Respondent has failed to demonstrate that the information it seeks is relevant.

The second prong of the *Shelton* factors requires that Respondent demonstrate both that the requested discovery is relevant and that the information sought is nonprivileged. Because Respondent has failed to demonstrate relevance, it is not necessary to determine whether Respondent has also demonstrated that the requested information is nonprivileged. Moreover, the record presented is insufficient to make such determination, and in such circumstances, it is inappropriate to resolve the issue. *See In re Gillette Co.*, 98 F.T.C. 875, 1981 FTC LEXIS 2, at *9 (Dec. 1, 1981) (reversing order denying application of informant's privilege where facts were insufficiently developed to "militate either in favor of overcoming or retaining the privilege," and remanding for further factual development).

C. Whether the information is crucial to the preparation of the case

Respondent argues that the requested information is crucial "to support its defenses that the Commission's actions toward LabMD are arbitrary, capricious, an abuse of discretion and in contravention of due process and fair notice." Opposition at 8. This conclusory assertion is unpersuasive. In any event, however, as shown above, Respondent has failed to demonstrate that the requested information is relevant, or that no other means exist to obtain the information. Having failed to demonstrate the first two of the three required *Shelton* factors, Respondent's effort to depose Mr. Sheer must fail. Accordingly, whether or not Respondent has met the third required prong by demonstrating that the information is crucial to the preparation of Respondent's case need not, and will not, be decided.

D. Policy considerations

Because Respondent has failed to meet its burden under *Shelton*, Respondent may not depose Mr. Sheer. Policy considerations further support applying *Shelton* to deny the requested deposition. As the court noted in *Sterne Kessler Goldstein & Fox, PLLC, v. Eastman Kodak Co.*, 276 F.R.D. 376, 380 (D.D.C. 2011), "[c]ourts confronted by demands for counsel depositions have noted a number of concerns that such discovery poses," including that:

> depositions of opposing counsel present a "unique opportunity for harassment." *Marco Island Partners v. Oak Dev. Corp.*, 117 F.R.D. 418, 420 (N.D. Ill. 1987); *see also Shelton*, 805 F.2d at 1330 ("The harassing practice of deposing opposing counsel (unless that counsel's testimony is crucial and unique) appears to be an adversary trial tactic that does nothing for the administration of justice but rather prolongs and increases the costs of litigation, demeans the profession, and constitutes an abuse of the discovery process."); . . . [In addition, t]ime involved in preparing for and undergoing such depositions will disrupt counsels' preparation of parties' cases and thus decrease the overall quality of representation. *See In re Subpoena Issued to Dennis Friedman*, 350 F.3d 65, 70 (2d Cir. 2003) ("Courts have been especially concerned about the burdens imposed on the adversary process when lawyers themselves have been the subject of discovery requests, and have resisted the idea that lawyers should routinely be subject to broad discovery."); *Shelton*, 805 F.2d at 1327 (depositions of opposing counsel "not only disrupts the adversarial system and lowers the standards of the profession, but it also adds to the already burdensome time and costs of litigation."); *Jennings v. Family Mgmt.*, 201 F.R.D. 272, 276-77 (D.D.C. 2001) ("[C]ourts regard attorney depositions unfavorably because they may interfere with the attorney's case preparation and risk disqualification of counsel who may be called as witness."); . . . . [Also] such depositions may lead to the disqualification of counsel who may be called as witnesses. *See Marco Island*, 117 F.R.D. at 420; *Jennings*, 201 F.R.D. at 276-77.

Sterne, 276 F.R.D. at 381-82.

In the instant case, permitting the requested deposition of Mr. Sheer implicates each of the foregoing concerns. Where, as here, it does not appear that Mr. Sheer possesses unique and/or crucial information, allowing the requested deposition risks disrupting trial preparation, increasing time and cost requirements, and countenancing potentially harassing trial tactics.

E. Protective Order

In addition to an order quashing the Sheer deposition subpoena, Complaint Counsel seeks an order barring Respondent from issuing any deposition subpoenas to Complaint Counsel generally. The burden of demonstrating an entitlement to this protective order is on Complaint Counsel. *In re Polypore Int'l*, 2008 FTC LEXIS 155, at *14-16 (Nov. 14, 2008); *In re Schering-Plough Corp.*, 2001 FTC LEXIS 105, at *5 (July 6, 2001).

It cannot be determined on the present record that the requested protective order is warranted. Complaint Counsel does not contend that Respondent has issued any deposition subpoenas to Complaint Counsel other than that issued to Mr. Sheer. Moreover, as noted earlier, attorneys are not immune from being deposed. *Shelton*, 805 F.2d at 1327. Rather, as is clear from *Shelton* and related authorities, the determination of whether a counsel deposition can proceed is a fact-based inquiry. Complaint Counsel's invitation to issue a "blanket" prohibition against future subpoenas directed to yet-to-be determined counsel is declined.

Because Complaint Counsel has failed to meet its burden of demonstrating an entitlement to the requested protective order, Complaint Counsel's Motion for a Protective Order is DENIED.

IV. Conclusion

For all the foregoing reasons, Complaint Counsel's Motion is GRANTED IN PART, and it is hereby ORDERED that Respondent's subpoena *ad testificandum* served on Complaint Counsel Alain Sheer is QUASHED. In all other respects, including Complaint Counsel's request for a protective order, the Motion is DENIED.

ORDERED:

D M Chappell

D. Michael Chappell
Chief Administrative Law Judge

Date: January 30, 2013

ORIGINAL

PUBLIC

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.

3) "[s]ince at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks." Complaint ¶ 16.

Respondent's Answer denies that Respondent violated the FTC Act or that any consumer was injured by the alleged security breach. Answer ¶¶ 17-23. Respondent's Answer asserts a number of affirmative defenses, including:

1) "Section 5 of the FTC Act does not give the Commission statutory authority to regulate the acts or practices alleged in the Complaint and therefore the Commission's actions are arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; contrary to constitutional right, power, privilege, or immunity; in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; or without observance of procedure required by law." Third Defense, Answer at p. 6; and

2) "[B]ecause the Commission has not published any rules, regulations, or other guidelines clarifying and providing notice, let alone constitutionally adequate notice, of what data-security practices the Commission believes Section 5 of the FTC Act forbids or requires and has not otherwise established any meaningful standards, this enforcement action against LabMD violates the due process requirements of fair notice and appropriate standards for enforcement guaranteed and protected by the Fifth Amendment to the U.S. Constitution and the Administrative Procedure Act." Fifth Defense, Answer at p. 7.

Respondent seeks a Rule 3.36 subpoena to obtain the following four categories of documents:

1) all communications to, from, or between FTC employees and the Commissioners relating to the 1718 file and the Sacramento Incident;

2) all communications to, from, or between FTC employees and the FTC's Office of Public Affairs relating to LabMD, the 1718 file, or the Sacramento Incident;

3) all documents sufficient to show the standards 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; and

4) all documents sufficient to show that since 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.

For each of these four categories, Respondent seeks production of documents for the time period of January 1, 2005 through the present, except to the extent that the documents are protected by privilege. Motion at 2.

II. Relevant Rules of Practice

Under Rule 3.36(a) of the Commission's Rules of Practice:

> An application for issuance of a subpoena for the production of documents, as defined in § 3.34(b), or for the issuance of a request requiring the production of or access to documents, other tangible things, or electronically stored information for the purposes described in § 3.37(a), in the possession, custody, or control of the Commissioners, the General Counsel, any Bureau or Office not involved in the matter, the office of Administrative Law Judges, or the Secretary in his or her capacity as custodian or recorder of any such information, or their respective staffs . . . , or for the issuance of a subpoena requiring the appearance of a Commissioner, the General Counsel, an official of any Bureau or Office not involved in the matter, an Administrative Law Judge, or the Secretary in his or her capacity as custodian or recorder of any such information, or their respective staffs, . . . shall be made in the form of a written motion filed in accordance with the provisions of § 3.22(a).

16 C.F.R. § 3.36(a).

Under Rule 3.36(b) of the Commission's Rules of Practice, a motion seeking the issuance of a 3.36(a) subpoena for purposes of discovery must demonstrate that the material sought is reasonable in scope, falls within the limits of discovery under § 3.31(c)(1), and cannot reasonably be obtained by other means; and that the subpoena meets the requirements of § 3.37.[2] 16 C.F.R. § 3.36(b).

Production of documents in discovery is also governed by Rule 3.31(c)(2), which provides:

> Complaint counsel need only search for materials that were collected or reviewed in the course of the investigation of the matter or prosecution of the case and that are in the possession, custody or control of the Bureaus or Offices of the Commission that investigated the matter, including the Bureau of Economics. The Administrative Law Judge may authorize for good cause additional discovery of materials in the possession, custody, or control of those Bureaus or Offices, or authorize other discovery pursuant to § 3.36. Neither complaint counsel, respondent, nor a third party receiving a discovery request under these rules is required to search for materials generated and transmitted between an entity's counsel (including counsel's legal staff or in-house counsel) and not shared with anyone else, or between complaint counsel and non-testifying Commission employees, unless the Administrative Law Judge determines there is good cause to provide such materials.

16 C.F.R. § 3.31(c)(2).

[2] Rule 3.37 governs production of documents and electronically stored information. 16 C.F.R. § 3.37.

III. Analysis

A. Communications to, from, or between FTC employees and the Commissioners relating to the 1718 file and the Sacramento Incident

To support the issuance of a Rule 3.36 subpoena for communications to, from, or between FTC employees and the Commissioners relating to the 1718 file and the Sacramento Incident, Respondent asserts that it assumes that Complaint Counsel will be required to prove that LabMD's data security was inadequate relevant to the 1718 file and the Sacramento Incident, and that Complaint Counsel will be required to present the data security standards that Complaint Counsel asserts LabMD violated. Respondent further asserts that "[c]ommunications to, from, or between the FTC and the Commissioners will show the type of information the Commissioners evaluated and considered prior to filing the complaint, and the data security standards that were used to determine that a complaint should be filed against LabMD." Motion at 5. Respondent thus asserts that such communications are relevant to its defense that the Commission's action in the issuance of the Complaint was arbitrary and capricious.

Complaint Counsel responds that discovery on Respondent's arbitrary and capricious defense has been precluded by the January 30, 2014 Order Granting Complaint Counsel's Motion to Quash Subpoena Served on Complaint Counsel and for Protective Order ("January 30 Order"). Additionally, Complaint Counsel asserts, Rule 3.31(c)(2) creates a default rule that materials generated and transmitted between Complaint Counsel and non-testifying Commission employees are not discoverable absent a ruling that there is good cause to provide these materials.

Discovery in adjudicative proceedings is limited to information that "may be reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses of any respondent." 16 C.F.R. 3.31(c)(1). By seeking to discover "the type of information the Commissioners evaluated and considered prior to filing the complaint," including the standards that the Commissioners used in determining whether to issue a complaint (Motion at 5), Respondent seeks information that is outside the scope of discovery, absent extraordinary circumstances.[3] January 30 Order. *E.g.*, *In re Metagenics, Inc.*, 1995 FTC LEXIS 23, *1 (Feb. 2, 1995) (denying as irrelevant discovery that related to respondent's claim that it had been unfairly singled out for prosecution); *In re Basic Research LLC*, 2004 FTC LEXIS 210, *10-11 (Nov. 4, 2004) (denying discovery, stating, "the issue to be tried is whether Respondent disseminated false and misleading advertising, not the Commission's decision to file the Complaint"). *See also In re Synchronal Corp.*, 1992 FTC LEXIS 61, *5 (March 5, 1992) (striking affirmative defense that the investigation was not in the public interest and was the result of selective prosecution as irrelevant and noting "[p]rejudice would occur from time and money spent in defending this irrelevant defense"). Once the Commission has issued a

[3] Although applicable precedent holds that the Commission's decision making in issuing a complaint is outside the scope of discovery in the ensuing administrative litigation, the Supreme Court has held that issuance of a complaint is reviewable on appeal of any resulting cease and desist order and noted that the FTC Act expressly authorizes a court of appeals to order that the Commission take additional evidence. *FTC v. Standard Oil Co. of California*, 449 U.S. 232, 245-46 (1980) (citing 15 U.S.C. § 45(c) and stating that "a record which would be inadequate for review of alleged unlawfulness in the issuance of a complaint can be made adequate"). Thus, limiting Respondent's discovery as provided herein does not prejudice Respondent's ability to pursue its claim at a later phase of the case.

complaint, "only in the most extraordinary circumstances" will the Commission review its reasons for issuing a complaint. *In re Boise Cascade Corp.*, 97 F.T.C. 246, 1981 FTC LEXIS 71, at *3 n.3 (March 27, 1981) (citing *TRW Inc.*, 88 F.T.C. 544 (1976)); *In re Exxon Corp.*, 83 F.T.C. 1759, 1974 FTC LEXIS 226 (June 4, 1974). Respondent has not presented "extraordinary circumstances" to obtain discovery on the type of information the Commissioners evaluated and considered prior to filing the complaint.

In addition, Commission Rule 3.31(c)(2) excludes from discovery, materials "between complaint counsel and non-testifying Commission employees, unless the Administrative Law Judge determines there is good cause to provide such materials." 16 C.F.R. § 3.31(c)(2). Respondent has not shown good cause to support its request for discovery from the Commissioners on the Commission's reasons for issuing the Complaint.

Therefore, with respect to all communications to, from, or between FTC employees and the Commissioners relating to the 1718 file and the Sacramento Incident, Respondent has not made the required showing for issuance of a Rule 3.36 subpoena.

B. Communications to, from, or between FTC employees and the FTC's Office of Public Affairs relating to LabMD, the 1718 file, or the Sacramento Incident

To support the issuance of a Rule 3.36 subpoena for communications to, from, or between FTC employees and the FTC's Office of Public Affairs, Respondent asserts: "[t]he FTC through its Office of Public Affairs has published disparaging statements in the media about LabMD which have had a negative commercial impact on the company" and that "[i]t is LabMD's position that these statements were published in retaliation for statements made by LabMD's CEO Michael Daugherty [who] criticized the FTC's investigation of LabMD's data security practices." Motion at 3. Respondent further states that the requested communications are relevant to show that the FTC violated Daugherty's First Amendment rights by retaliating against LabMD for speech criticizing the FTC's actions. *Id.*

Complaint Counsel responds that Respondent has not asserted a First Amendment defense in this administrative proceeding. Instead, Complaint Counsel asserts, Mr. Daugherty's First Amendment claims are the subject of a separate lawsuit, *LabMD v. FTC*, 13-cv-01787 (D.D.C. filed Nov. 14, 2013).[4] Complaint Counsel further asserts that, to the extent that Respondent is attempting to tie its First Amendment claims to its Third Defense, discovery on such matter has been precluded by the January 30 Order. Additionally, Complaint Counsel asserts that Respondent has not shown good cause to abrogate the default rule set forth in Rule 3.31(c)(2) that materials generated and transmitted between Complaint Counsel and non-testifying Commission employees are not discoverable.

[4] In its complaint against the FTC in federal district court, LabMD alleges that the FTC learned of Mr. Daugherty's criticisms of the FTC and retaliated against LabMD through the issuance of this administrative complaint. *LabMD v. FTC*, 13-cv-01787 (D.D.C. Complaint ¶¶ 13-16, filed Nov. 14, 2013). On February 19, 2014, LabMD filed a Notice of Voluntary Dismissal Without Prejudice in that action.

Documents that may be reasonably expected to show whether or not "the FTC violated Daugherty's First Amendment rights by retaliating against LabMD" in filing this Complaint are not relevant to the allegations of the Complaint, the proposed relief, or the defenses of Respondent. A careful review of Respondent's Answer shows that the Answer does not assert such a defense. Accordingly, the requested material does not fall within the limits of discovery under § 3.31(c)(1). Furthermore, as analyzed above, discovery on the Commission's reasons for issuing a complaint is improper, absent extraordinary circumstances.

In addition, Commission Rule 3.31(c)(2) excludes from discovery, materials "between complaint counsel and non-testifying Commission employees, unless the Administrative Law Judge determines there is good cause to provide such materials." 16 C.F.R. § 3.31(c)(2). Respondent's claim, that the FTC's filing of this administrative complaint was in retaliation for Mr. Daugherty's exercise of his First Amendment rights, does not provide "good cause" for discovery in this administrative adjudication.

Therefore, with respect to communications to, from, or between FTC employees and the FTC's Office of Public Affairs, Respondent has not made the required showing for issuance of a Rule 3.36 subpoena.

C. Documents on standards the FTC uses to evaluate entities' data-security practices

To support the issuance of a Rule 3.36 subpoena for all documents sufficient to show the standards 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, Respondent asserts that such documents will show the standards that the Commission utilized in determining to bring a complaint against LabMD. Motion at 4. Respondent also asserts that such documents are relevant to its defense that the Commission's behavior toward LabMD was "arbitrary, capricious, an abuse of discretion, and otherwise not in accordance with the law." Motion at 4. Respondent further asserts that because the Commission failed to publish rules, regulations, and guidelines constituting fair notice, this information is relevant and necessary to determine whether the Complaint was issued in order to retaliate against Daugherty for exercising his First Amendment rights in criticizing the FTC.

Complaint Counsel responds that this request relates to Respondent's Third Defense and Fifth Defense. Complaint Counsel argues that the Commission's January 16, 2014, Order Denying Respondent LabMD's Motion to Dismiss (January 16 Commission Order) and the January 30 Order on Complaint Counsel's Motion for Protective Order foreclosed discovery on these topics.

Respondent's arguments in support of obtaining this category of documents mirror its arguments for obtaining documents addressed above in Parts III.A. and B. For the reasons stated above, Respondent's request for documents to show: the standards that the Commission utilized in determining to bring a complaint against LabMD; that the Commission's behavior towards LabMD was "arbitrary and capricious"; and that the issuance of the Complaint was motivated by

retaliation for Daugherty's exercise of his First Amendment rights, are all matters that are outside the scope of permissible discovery in this case.

Therefore, for the reasons set forth in Parts III.A and B, above, with respect to the request for all documents sufficient to show the standards the FTC used in the past and is currently using to determine whether an entity's data security practices violate Section 5 of the FTC Act, Respondent has not made the required showing for issuance of a Rule 3.36 subpoena.

D. Documents sufficient to show that since 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks

To support the issuance of a Rule 3.36 subpoena for documents to show that since 2005, security professionals and the Commission have warned of the risks of P2P networks, Respondent asserts that "Complaint Counsel, by the drafting of its own Complaint, calls into question whether the Commission has warned that P2P applications present a risk." Motion at 4. Complaint Counsel does not address this argument, but instead focuses on whether the requested discovery is relevant to Respondent's Fifth Defense that "the Commission has not published any rules, regulations, or other guidelines clarifying and providing any notice . . . of what data-security practices the Commission believes Section 5 of the FTC Act forbids" ("fair notice defense") and asserts that the January 16 Commission Order foreclosed discovery into Respondent's fair notice defense. Opposition at 6.

Regardless of whether, in denying Respondent's Motion to Dismiss for failure to provide fair notice of applicable security standards, the Commission "precluded" discovery on Respondent's fair notice defense, the Complaint specifically avers, "[s]ince at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks." Complaint ¶ 16. Thus, documents sufficient to show that since 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks are relevant to the allegations of the Complaint and therefore fall within the limits of discovery under Rule 3.31(c)(1).

While Respondent has demonstrated that the requested documents are relevant to the allegations of the Complaint, it has not met the requirement of Rule 3.36(b)(3) that the information sought cannot reasonably be obtained by other means. 16 C.F.R. § 3.36(b)(3), as Respondent has failed to demonstrate why it cannot obtain this information directly from Complaint Counsel. Indeed, Complaint Counsel states that it has produced 9,966 pages of documents consisting of publications and statements of the Commission and its staff relating to the dangers posed by P2P file-sharing and to data security, including cases, business and consumer education, testimony before Congress and state agencies, speeches, staff reports, and workshop materials.

To the extent it has not already done so in response to discovery requests served upon it, Complaint Counsel is ordered to "search for materials that were collected or reviewed in the course of the investigation of the matter or prosecution of the case and that are in the possession,

custody, or control of the Bureaus or Offices of the Commission that investigated the matter, including the Bureau of Economics" (16 C.F.R. § 3.31(c)(2)) relevant to the Complaint's allegation that, since 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks, and to produce non-privileged, responsive materials within 14 days.[5] Complaint Counsel is not required to produce materials "between complaint counsel and non-testifying Commission employees," as Respondent has not provided any basis for finding that good cause exists to require such production. 16 C.F.R. § 3.31(c)(2).

With respect to documents sought from employees of the Commission not involved in the matter, Respondent has not made the required showing for issuance of a Rule 3.36 subpoena.

IV. Conclusion

For all the foregoing reasons, Respondent's Motion for a Rule 3.36 Subpoena is DENIED.

ORDERED:

D M Chappell

D. Michael Chappell
Chief Administrative Law Judge

Date: February 21, 2014

[5] Complaint Counsel will be precluded from offering into evidence in this matter any responsive documents or other information not produced that relate to or might support the allegations in paragraph 16 of the Complaint.

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 GRANTING COMPLAINT COUNSEL'S MOTION TO QUASH AND TO LIMIT DEPOSITION SUBPOENAS SERVED ON COMMISSION ATTORNEYS

On February 10, 2014, Complaint Counsel filed a Motion to Quash Subpoena Served on Commission Attorney Carl Settlemyer and to Limit Subpoena Served on Commission Attorney Ruth Yodaiken ("Motion"). Respondent LabMD, Inc. ("Respondent" or "LabMD") filed an opposition to the Motion on February 20, 2014 ("Opposition").

Having fully reviewed the Motion and the Opposition, and considered all arguments and contentions raised therein, the Motion is GRANTED, 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 Federal Trade Commission ("FTC") Act. Complaint ¶ 23. Specifically, the Complaint alleges that Respondent failed to maintain adequate network security to protect confidential patient information, including by making certain "insurance aging reports," allegedly containing confidential patient information, available on a peer-to-peer, or "P2P" file sharing application ("the 1718 file"). Complaint ¶¶ 17, 19. The Complaint further avers that in October 2012, the Sacramento, California Police Department ("SPD") found more than 35 LabMD "Day Sheets," allegedly containing confidential patient information ("Day Sheets"),[1] and a small number of copied checks, in the possession of individuals who subsequently pleaded no contest to state charges of identity theft (the "Sacramento Incident"). Complaint ¶ 21.

Respondent's Answer admits that an alleged third party, Tiversa Holding Corporation ("Tiversa"), contacted Respondent in May 2008 and claimed to have obtained the P2P insurance aging file via LimeWire, but denies that Respondent violated the FTC Act or that any consumer

[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.

was injured by the alleged security breach. Answer ¶¶ 17-23. Respondent's Answer also includes a number of affirmative defenses, including among others, failure to state a claim, lack of subject matter jurisdiction, denial of due process and fair notice, and that the actions of the FTC are arbitrary, capricious, an abuse of discretion, and otherwise not in accordance with applicable law. Answer at pp. 6-7.

On January 30, 2014, Respondent served two subpoenas *ad testificandum*, one directed to FTC attorney Carl Settlemyer and one directed to FTC attorney Ruth Yodaiken. Complaint Counsel seeks to quash the Settlemyer subpoena in its entirety and to limit the Yodaiken subpoena to the topic of the substance of Ms. Yodaiken's communications with the SPD. Motion at 1.

II. Scope of Discovery

Under Rule 3.31(c)(1), "[p]arties may obtain discovery to the extent that it may be reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses of any respondent." 16 C.F.R. § 3.31(c)(1).

As set forth in the Orders of January 30, 2014 and February 21, 2014, issued in this case, once an administrative complaint is issued, the decision making process preceding such issuance is not discoverable in the ensuing litigation absent extraordinary circumstances. Order of January 30, 2014 at 5-6, citing *In re Exxon Corp.*, 83 F.T.C. 1759, 1974 FTC LEXIS 226, at *2-3 (June 4, 1974) ("Once the Commission has resolved these questions and issued a complaint, the issue to be litigated is not the adequacy of the Commission's pre-complaint information or the diligence of its study of the material in question but whether the alleged violation has in fact occurred."); *In re Boise Cascade Corp.*, 97 F.T.C. 246, 1981 FTC LEXIS 71, at *3 n.3 (March 27, 1981) (holding that once a complaint issues, the Commission's determinations in issuing the complaint are reviewed "only in the most extraordinary circumstances"); Order of February 21, 2014 (denying Respondent's Motion for Issuance of Rule 3.36 Subpoena to obtain communications to, from, or between FTC employees and the Commissioners relating to the 1718 file and the Sacramento Incident, in part based upon *Boise/Exxon* Rule). *See also In re Exxon Corp.*, 1981 FTC LEXIS 113, at *5-6 (Jan. 29, 1981) (denying on relevance grounds respondent's renewed request for discovery into whether the Commission had "reason to believe" that a violation of law had occurred); *In re Basic Research LLC*, 2004 FTC LEXIS 210, *10-11 (Nov. 4, 2004) (denying as not relevant discovery into the Commission's decision to file the complaint); *In re Metagenics, Inc.*, 1995 FTC LEXIS 23, *1 (Feb. 2, 1995) (denying as irrelevant discovery of documents that "led up to the complaint" and discovery related to respondent's claim that it had been unfairly singled out for prosecution).

Respondent asserts that "[i]t is believed that both [Mr. Settlemyer and Ms. Yodaiken] were FTC employees involved with: (1) FTC's handling of LabMD's property when importuned from the [SPD]; (2) FTC's interactions with Tiversa . . . preceding this adjudication, including but not limited to Tiversa's possession and transmittal of LabMD [documents] to the FTC; and, (3) communications involving Dartmouth College's (Dartmouth) data security study," which Respondent identifies as "Data Hemorrhages in the Health-Care Sector, Dartmouth College," by M. Eric Johnson, Presented at Financial Cryptography and Data Security, Feb. 22-25, 2009

(available at http: //cds.tuck.dartmouth.edu/cds- uploads/researchprojects/pdf/Johnson HemorrhagesFC09Proceedingd.pdf). Opposition at 1-2. Respondent states, *inter alia*, that "Settlemyer was a point of contact for FTC's interactions with Tiversa and Dartmouth (Compl. Mot. Ex. F). Settlemyer corresponded with Tiversa regarding Tiversa's report on the release of Protected Health Information (PHI). (Compl. Mot. Ex. F). Settlemyer was party to e-mails with Eric Johnson of Dartmouth regarding Mr. Johnson's paper on PHI [Protected Health Information]. (Attached as Ex. 2)." Opposition at 2. Complaint Counsel represents that Mr. Settlemyer had no communications with SPD, and that Ms. Yodaiken had no communications with either Tiversa or Dartmouth College.

Respondent contends that notwithstanding the fact that Mr. Settlemyer and Ms. Yodaiken are FTC attorneys, they may be deposed in this case because they are "fact witnesses," citing *In re Hoechst Marion Roussel, Inc.*, 2000 WL 33944050, at *1 (Nov. 8, 2000) (stating that deposition of counsel is "permissible where the attorney is a fact witness . . . . [W]here the attorney's conduct itself is the basis of a claim or defense, there is little doubt that the attorney may be examined as any other witness"). Putting aside the fact that discovery was denied in *Hoechst* for failure to demonstrate that the subject FTC attorneys and staff member had any relevant knowledge, the cited rule is not being challenged in this Motion. Complaint Counsel does not argue that Mr. Settlemyer or Ms. Yodaiken are immune from deposition, or even that these individuals' status as FTC attorneys requires application of a higher standard to allow such discovery, such as that applicable to a deposition of a party's litigation counsel. *See Shelton v. Am. Motors Corp.*, 805 F.2d 1323, 1327 (8th Cir. 1986) (holding that a party seeking deposition of a party's litigation counsel must show: "(1) no other means exist to obtain the information than to depose opposing counsel, . . . ; (2) the information sought is relevant and nonprivileged; and (3) the information is crucial to the preparation of the case"). Rather, the issue here is whether Mr. Settlemyer and Ms. Yodaiken have knowledge of facts that are themselves relevant, or will likely lead to the discovery of relevant evidence, pursuant to Rule 3.31(c)(1).

III. Deposition Subpoena to FTC Attorney Settlemyer

A. Communications with Tiversa

It appears from the undisputed representations of the parties and from the exhibits attached to the Motion and Opposition that Mr. Settlemyer is an attorney in the FTC's Bureau of Consumer Protection, Division of Advertising Practices. On June 25, 2008, Mr. Settlemyer sent a letter to Tiversa advising that the FTC had received a request for information from a congressional committee, to which certain materials Tiversa had submitted may be responsive, and that Tiversa's submissions may be disclosed pursuant to that request. (Motion Ex. E). Furthermore, on January 26, 2009, Mr. Settlemyer contacted Tiversa by email, with the subject line "P2P ID Theft Research – Conference Call?", requesting a conference call between Tiversa representatives and FTC representatives to discuss a then-recent press release issued by Tiversa. A series of scheduling emails were exchanged over the next 6 weeks, culminating on March 4, 2009, with an agreement to a conference call for March 5, 2009. (Motion Ex. F). Robert Boback, Chief Executive Officer of Tiversa, testified at his deposition that he had two meetings with FTC representatives in early 2009, one in Pittsburgh and one at the FTC headquarters in Washington, D.C. Mr. Boback did not recall Mr. Settlemyer personally. He further stated that

only Senior Complaint Counsel Mr. Alain Sheer and an unidentified woman attended the Pittsburgh meeting, and that LabMD was not discussed at this meeting. (Opposition Ex. 4 (Dep. of Robert Boback 138-141, 145)). As to the Washington, D.C. meeting, Mr. Boback was unable to recall any attendees other than Mr. Sheer and the unidentified woman. He further testified that LabMD might have been discussed at the Washington, D.C. meeting, but not for any extended time and no more than any other organizations that were discussed. (*Id.*).

Complaint Counsel argues that Mr. Settlemyer's communications with Tiversa are beyond the scope of discovery under Rule 3.31(c)(1) because the Commission's decision making with regard to issuing the Complaint is not relevant. Complaint Counsel further contends that these communications constitute "materials" that were not "collected or reviewed in the course" of the investigation of LabMD or the prosecution of this case, and are therefore protected from discovery by Rule 3.31(c)(2), absent a showing of good cause.[2]

Respondent's Opposition fails to properly articulate or persuasively explain why communications between an FTC staff attorney and Tiversa, prior to the commencement of the investigation of LabMD, are themselves relevant, or are reasonably calculated to lead to the discovery of relevant evidence. For example, Respondent states that "the Civil Investigative Demand [CID] which resulted in the production of Tiversa's documents to FTC was served on a third party other than Tiversa. Settlemyer is likely to have knowledge of this unusual arrangement. (Dep. of Robert Boback 142-143, Nov. 21, 2013, attached as Ex. 4)." Opposition at 4. In the cited testimony, Mr. Boback explains that Tiversa was at that time being considered for acquisition; that he did not want Tiversa to be "under" a CID; and that in order to create some "distance" between Tiversa and the CID, the CID was provided to a third party, the "Privacy Institute," and "funneled" to Tiversa which then produced the requested documents to the Privacy Institute, which in turn provided Tiversa's responsive documents to the FTC. Even if it is assumed for purposes of argument that the method by which Tiversa provided documents to the FTC can be characterized as "unusual," Respondent fails to articulate how additional discovery on the topic relates to any claim or defense in this case. Similarly, Respondent argues, Mr. Boback could not recall a conference call or meeting that was referenced in Mr. Settlemyer's emails of February and March 2009, and, therefore, Respondent needs to obtain the information from Mr. Settlemyer. Yet, again, Respondent fails to articulate how the substance of such call or meeting pertains to any claim or defense. To the extent that Respondent seeks to discover the FTC's communications with Tiversa in order to challenge the Commission's actions, processes, or decision making leading up to the issuance of the Complaint in this case, "[p]recedent dictates that such matters are not relevant for purposes of discovery in an administrative adjudication." Order of January 30, 2014, at 6. Indeed, that Order, applying the *Exxon* rule, specifically denied discovery of pre-Complaint attorney communications with Tiversa on the ground, *inter alia*, that such communications are not relevant to this case. *See also* Order of February 21, 2014 (denying Respondent's Request for Issuance of Rule 3.36 Subpoena in part on the basis of the *Exxon* rule).

---

[2] Rule 3.31(c)(2) states, in pertinent part, absent a showing of good cause,"[c]omplaint counsel need only search for materials that were collected or reviewed in the course of the investigation of the matter or prosecution of the case . . . ." 16 C.F.R. § 3.31(c)(2).

Accordingly, based on the foregoing, the Tiversa-related information that Respondent seeks from Mr. Settlemyer is beyond the scope of permissible discovery under Rule 3.31(c)(1).

B. Communications with Professor Eric Johnson

It appears from the undisputed representations of the parties and from the exhibits attached to the Motion and Opposition that on February 3, 2009, Mr. Settlemyer contacted Professor Eric Johnson of Dartmouth College by email, with the subject line "New Article," requesting a copy of Professor Johnson's "new article coming out concerning health info available on P2P networks . . . . As you know from our past discussions, this is an area of interest to us [and the article] sounds like . . . a significant expansion of your prior work." (Opposition Ex. 2). Professor Johnson proceeded to send the article to Mr. Settlemyer. (*Id.*). A series of emails followed that transmission, with the subject line, "Health Care Data Leaks via P2P," to arrange a conference call among Mr. Johnson, Mr. Settlemyer, and Mr. Sheer for March 12, 2009.

Complaint Counsel contends that Respondent seeks to discover Mr. Settlemyer's communications with Dartmouth College in order to litigate the adequacy of the FTC's pre-Complaint process, and that, therefore, these communications are not relevant under the *Exxon* rule, summarized above, and previously applied to discovery disputes in this case in the Orders of January 30 and February 21, 2014. Complaint Counsel further argues that any such communications constitute "materials" that were not "collected or reviewed in the course" of the investigation or prosecution in this case, and are therefore barred from discovery under Rule 3.31(c)(2). In addition, Complaint Counsel contends, even if Mr. Settlemyer's communications with Dartmouth were relevant, Respondent does not need to depose Mr. Settlemyer on such communications because it can obtain the information from a representative from Dartmouth, pursuant to Respondent's issuance of a deposition subpoena on January 30, 2014.

Complaint Counsel states that it does not intend to call Mr. Settlemyer as a witness, and Professor Johnson has not been included as a potential witness on Complaint Counsel's Preliminary Witness List. However, the Motion does not state whether or not Complaint Counsel plans to rely at trial upon Professor Johnson's article regarding health care data leaks. Nor does Complaint Counsel assert that Professor Johnson possesses no relevant knowledge. In any event, even if the article and Mr. Johnson's related testimony may be relevant in this matter, Respondent fails to articulate why or how Mr. Settlemyer's *communications* with Mr. Johnson pertain to any claim or defense. Moreover, the Order of January 30, 2014, relying on the *Exxon* rule, rejected Respondent's argument that the FTC's pre-Complaint communications with, *inter alia*, Dartmouth College are discoverable to show that "the Commission's actions in investigating and filing a complaint" in this matter were contrary to law, as claimed by Respondent in its Answer. Order of January 30 at 5-6.

For all the foregoing reasons, deposition testimony from Mr. Settlemyer regarding FTC communications with Dartmouth College is beyond the permissible scope of discovery under Rule 3.31(c)(1).

C. Communications with SPD

Finally, Complaint Counsel represents that Mr. Settlemyer had no communications with SPD, and that Respondent has been advised accordingly. Respondent does not dispute this representation, and there is nothing in the record presented to contradict Complaint Counsel's assertion. Accordingly, there is no basis for permitting the deposition for the purpose of discovering such communications.

In summary, because it does not appear that any of Respondent's proposed discovery from Mr. Settlemyer is relevant, or reasonably calculated to lead to the discovery of relevant evidence, Complaint Counsel's Motion to Quash the subpoena to Mr. Settlemyer is GRANTED.[3]

IV. Deposition Subpoena to FTC Attorney Yodaiken

According to Complaint Counsel, Ms. Yodaiken participated in the Commission's investigation of LabMD from January 2010 through July 2013. Complaint Counsel states that in February 2013, Ms. Yodaiken represented the Commission at two investigational hearings in this matter, conducting the examination of LabMD President and Chief Executive Officer Michael J. Daugherty. Ms. Yodaiken has not entered an appearance in this litigation.

The record presented shows that Ms. Yodaiken was a party to conversations with SPD regarding the Sacramento Incident, including with regard to the transmittal of LabMD documents to the FTC and arrangements for contacting consumers whose information appeared on the LabMD documents confiscated by SPD as part of the Sacramento Incident. Complaint Counsel states that it identified Ms. Yodaiken in its Response to Respondent's First Set of Interrogatories as an "individual[] at the FTC who communicated with" the SPD regarding the Sacramento Incident. *See also* Opposition Ex. 3 (Dep. of Detective Karina Jestes, Dec. 17, 2013, 65-67). Complaint Counsel does not object to producing Ms. Yodaiken for a deposition limited to the topic of such communications. For all these reasons, Respondent is entitled to depose Ms. Yodaiken as to the substance of her communications with SPD.

Complaint Counsel states that Ms. Yodaiken has not had any communications with Tiversa or Dartmouth College, and that Respondent has been advised accordingly. Respondent asserts, however, that Ms. Yodaiken may have been a party to correspondence and meetings with Tiversa and Dartmouth because Ms. Yodaiken "customarily" works with Mr. Sheer; was a contact on a CID issued to LabMD; and may be the unidentified woman who, along with Mr. Sheer, attended the 2009 Pittsburgh and Washington, D.C. meetings with Tiversa. Opposition at 6. However, when specifically asked at his deposition if Ms. Yodaiken was the woman present at these meetings, Mr. Boback responded, "It may have been her . . . I don't know her name at all." The foregoing is insufficient to conclude that Ms. Yodaiken communicated with Tiversa and Dartmouth, considering the representation of Complaint Counsel that Ms. Yodaiken has not had any communications with Tiversa or Dartmouth. In addition, as noted above, to the extent

---

[3] Because the requested communications with Tiversa and Dartmouth are beyond the scope of discovery under the *Exxon* rule, it need not be determined whether such communications are also shielded from discovery under Rule 3.31(c)(2), as argued by Complaint Counsel.

that Respondent seeks to discover through Ms. Yodaiken the FTC's communications with Tiversa or Dartmouth in order to challenge the Commission's actions in investigating and filing the Complaint in this case, such pre-Complaint communications are not relevant, or reasonably likely to lead to the discovery of relevant evidence, and thus are not discoverable.

Based on the foregoing, Complaint Counsel's Motion to Limit the subpoena issued to Ms. Yodaiken to the topic of Ms. Yodaiken's communications with SPD is GRANTED.

V. Conclusion

Based on full consideration of the Motion and Opposition, and for all the foregoing reasons, Complaint Counsel's Motion is GRANTED, and it is hereby ORDERED that (1) the subpoena *ad testificandum* served on Carl Settlemyer is QUASHED, and (2) the subpoena *ad testificandum* served on Ruth Yodaiken is LIMITED to testimony about the substance of her communications with the Sacramento Police Department.[4]

ORDERED:

D M Chappell

D. Michael Chappell
Chief Administrative Law Judge

Date: February 25, 2014

[4] Moreover, as noted in the Order of February 21, 2014, limiting Respondent's discovery as provided herein does not prejudice Respondent's ability to pursue at a later phase of the case its claim that the Commission's actions in investigating and filing the Complaint were unlawful. *See FTC v. Standard Oil Co. of California*, 449 U.S. 232, 245-46 (1980).

Notice of Electronic Service

I hereby certify that on September 21, 2016, I filed an electronic copy of the foregoing RESPONDENT LabMD, INC.'S OPPOSITION TO COMPLAINT COUNSEL'S MOTION FOR LEAVE TO FILE SURREPLY , with:

D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Ave., NW
Suite 110
Washington, DC, 20580

Donald Clark
600 Pennsylvania Ave., NW
Suite 172
Washington, DC, 20580

I hereby certify that on September 21, 2016, I served via E-Service an electronic copy of the foregoing RESPONDENT LabMD, INC.'S OPPOSITION TO COMPLAINT COUNSEL'S MOTION FOR LEAVE TO FILE SURREPLY , upon:

John Krebs
Attorney
Federal Trade Commission
jkrebs@ftc.gov
Complaint

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Jarad Brown
Attorney
Federal Trade Commission
jbrown4@ftc.gov
Complaint

Kent Huntington
Counsel
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Sunni Harris
Esq.
Dinsmore & Shohl LLP
sunni.harris@dinsmore.com
Respondent

Daniel Epstein
Cause of Action
daniel.epstein@causeofaction.org
Respondent

Patrick Massari
Counsel
Cause of Action
patrick.massari@causeofaction.org
Respondent

Alain Sheer
attorney
Federal Trade Commission
asheer@ftc.gov
Complaint

Laura Riposo VanDruff
General Attorney
Federal Trade Commission
lvandruff@ftc.gov
Complaint

Megan Cox
Attorney
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Attorney
Federal Trade Commission
rmehm@ftc.gov
Complaint

Erica Marshall
Counsel
Cause of Action
erica.marshall@causeofaction.org
Respondent

Alfred Lechner
President & CEO
Cause of Action Institute
jlechner@causeofaction.org
Respondent

Patrick Massari
Attorney