

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



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

PUBLIC

Docket No. 9357

ORIGINAL

**COMPLAINT COUNSEL’S OPPOSITION TO
RESPONDENT’S MOTION FOR SANCTIONS**

Respondent’s Motion, which exceeds the applicable word limit and regarding which counsel never met-and-conferred with Complaint Counsel, seeks relief that the Commission’s Rules do not authorize. If there were a legal basis for Respondent’s relief, its baseless claims regarding Complaint Counsel’s evidence ignores its own admissions regarding practices that cause or are likely to cause substantial injury to consumers, including its admission that a 1,718-page LabMD document containing Social Security numbers, health information, and other sensitive personal information for more than 9,300 consumers (“1718 File”) was available for sharing through LimeWire installed on a LabMD computer.

BACKGROUND

On August 28, 2013, the Commission issued its Complaint alleging that Respondent LabMD, Inc.’s unreasonable data security practices violated Section 5 of the Federal Trade Commission Act. The Complaint followed a thorough investigation of LabMD’s data security practices, which Respondent stalled for nearly a year by refusing to comply with compulsory process. The Complaint alleges, *inter alia*, that LabMD’s systemic failure to provide reasonable and appropriate security for sensitive personal information on its computer networks constituted

an unfair practice under Section 5 of the Federal Trade Commission Act (“Section 5”). *E.g.*, Compl. ¶¶ 10-12, 22.

The pre-Complaint investigation, the adequacy of which is not at issue in this litigation,¹ included reviewing several thousand pages of documents produced by LabMD, conducting Investigational Hearings of LabMD’s designee, its president, and several of its former information technology (“IT”) employees, and evaluating documents provided by third parties, including documents produced by the Privacy Institute pursuant to the Commission’s Civil Investigative Demand.

In accordance with its Rule 3.31(b) obligations, Complaint Counsel disclosed these materials in its September 24, 2013 Initial Disclosures. **Ex. A** (confidential in part). Complaint Counsel’s Initial Disclosures included a copy of the 1718 File. CX0697. Contrary to Respondent’s suggestion that information regarding the Privacy Institute was withheld until November 2013, *see* Mot. at 7, Complaint Counsel’s Initial Disclosures noted specifically that the 1718 File and related documents had been “provided to the Commission by the Privacy Institute pursuant to compulsory process.” **Ex. A** at 3.

Fact discovery in this proceeding further demonstrated Respondent’s unlawful data security practices by documenting “acts of omission” and “acts of commission” in the company’s failures to protect consumers’ personal information. Order Den. Mot. to Dismiss (Jan. 16, 2014) at 18 (“MtD Order”); *see, e.g.*, JX0001, Fact 6 (admitting that LabMD did not memorialize security policies in writing until 2010); *id.*, Fact 8 (admitting that LabMD did not

¹ *See In re Exxon Corp.*, No. 8934, 1974 FTC LEXIS 226, at *2-3 (June 4, 1974) (“Once the Commission has . . . 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.”).

conduct penetration tests until 2010); *id.*, Fact 5 (admitting that LabMD maintained personal information about approximately 100,000 consumers for whom it never performed laboratory tests); CX0754 (admitting that LabMD cannot specify limits it placed on employees' access to personal information); CX0734 at 60-63 (LabMD provided no formal employee training regarding IT); CX0167 (identifying weak passwords); CX0067 at 22-23, 65 (identifying a critical vulnerability from failing to update an operating system). Respondent also admitted that LimeWire was installed on a LabMD computer, and hundreds of files on the computer, including the 1718 File, were available for sharing on a peer-to-peer ("P2P") network. JX0001, Facts 10-11.

In addition to Respondent's admissions, fact discovery also revealed that an information security firm, Tiversa, found the 1718 File at multiple Internet Protocol ("IP") addresses. CX0703 at 111; RX541 at 76. *Cf.* RX541 at 67 (no knowledge of Tiversa having downloaded the 1718 File from a workstation at LabMD). Following Respondent's counsel's *in camera* proffer of testimony Respondent anticipates former Tiversa employee Richard Wallace may provide if granted immunity, Complaint Counsel sought leave of Court to take additional discovery to refute his anticipated testimony and to demonstrate Mr. Wallace's bias.² In addition, Complaint Counsel obtained public records that corroborate Tiversa CEO Robert

² Contrary to Respondent's assertion, the Court did not determine that "there was no 'good cause to reopen discovery, at this late stage of the proceedings.'" Mot. at 2. Rather, the Court observed that "*on the present record, it cannot properly be determined* what might constitute permissible rebuttal or impeachment evidence, much less whether there is good cause to reopen discovery, at this late stage of the proceedings, to obtain such evidence." Order Den. Compl. Counsel's Mot. for Leave (July 23, 2014) at 2 (emphasis added).

Boback's June 7, 2014 testimony regarding Mr. Wallace.³ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Discharging any possible obligation to supplement its Initial Disclosures under Rule 3.31(e), Complaint Counsel supplied copies of the public records to Respondent on July 28, 2014.

Two weeks later, ignoring its obligations under Rule 3.22 and the Additional Provisions of this Court's Scheduling Order to meet-and-confer and limit its filing to 2,500 words, Respondent filed its Motion for Sanctions in response to Complaint Counsel's Motion for Leave to Issue Subpoenas for Rebuttal Evidence.

ARGUMENT

Respondent's Motion, which was filed improperly, fails for three reasons. First, the Commission's Rules of Practice do not authorize Respondent's sought relief. Second, Respondent's Motion obscures its admission that the 1718 File was available for sharing on a P2P network from a LabMD computer, a fact that itself establishes likely substantial consumer injury. Third, Respondent's Motion ignores admitted evidence amply demonstrating that LabMD engaged in unreasonable data security practices.

³ Respondent's repeated assertion that Mr. Wallace appears on Complaint Counsel's witness list, Mot. at 2, 5, is patently false. *See* Compl. Counsel's Prelim. Witness List (Dec. 19, 2013) (**Ex. B**); Compl. Counsel's Suppl. Prelim. Witness List (Feb. 27, 2014) (**Ex. C**); Compl. Counsel's Final Proposed Witness List (Mar. 26, 2014) (**Ex. D**).

I. RESPONDENT SEEKS IMPERMISSIBLE RELIEF**A. Commission Rules Do Not Authorize Requested Sanctions**

Respondent's Motion seeks extraordinary relief that the Commission's Rules of Practice do not authorize. As this Court observed in 2010 in ruling on a similar motion, "the Commission's Rules of Practice do not contain a rule analogous to Rule 11 of the Federal Rules of Civil Procedure." *In re Gemtronics, Inc.*, No. 9330, 2010 FTC LEXIS 40, at *8 (Apr. 27, 2010) (Order Denying Motion for Sanctions). Indeed, Respondent points to no Rule authorizing the Court to impose sanctions for the conduct alleged in its Motion.

B. Respondent's Motion Was Filed Improperly

If the Rules permitted such extraordinary relief, which they do not, the Court should nonetheless deny it here because Respondent failed to meet-and-confer or to limit its submission to 2,500 words, as required by the Rules of the Practice and the Scheduling Order of this Court. *See* Rule 3.22(c) (word limitation); Add'l Provisions, Sched. Order ¶¶ 4, 5 (Sept. 25, 2013) (meet-and-confer and word limitation).

II. LABMD ADMITS THAT ITS 1718 FILE WAS AVAILABLE FOR SHARING

Respondent's Motion fails because its own admissions establish that the 1718 File—which is the subject of Respondent's Motion—was available for sharing on a P2P network from a LabMD computer.⁴ A document that is available for sharing on a P2P network may be freely

⁴ *See, e.g.*, JX0001, Facts 10-11. More than 900 files on the LabMD computer, including the 1718 File, were available for sharing through LimeWire. *Id.*, Fact 11.

accessed by other users of the network.⁵ Accordingly, the availability of the 1718 File and the sensitive personal information for more than 9,300 consumers that it contains resulted in likely substantial consumer injury. *Accord* MtD Order at 19 (“[O]ccurrences of actual data security breaches . . . are not necessary to substantiate that the firm’s data security activities caused or likely caused consumer injury”); Comm’n Statement of Policy (Dec. 17, 1980), *reprinted in Int’l Harvester Co.*, No. 9147, 1984 FTC LEXIS 2, at *300, *308 n.12 (Dec. 21, 1984) (act or practice may cause “substantial injury” if it causes a “small harm to a large number of people” or “raises a significant risk of concrete harm”).

Moreover, undisputed evidence from Tiversa supports the conclusion that the availability of the 1718 File constituted likely substantial injury.⁶ Specifically, Tiversa found the 1718 File

⁵ *See, e.g.*, Trial Tr. at 862-63 (Professor Clay Shields stating that the 1718 File was available for sharing and that “[a]ny one of the millions of other [Gnutella] clients that were running on the Gnutella network could have downloaded this file”); *id.* at 1198 (Adam Fisk stating that any user who located the 1718 File could download it on the LimeWire network); *id.* at 762 (Dean Johnson analogizing a computer on a P2P network to a box with the word “free” written on its side).

⁶ Tiversa received no government funds for the work it performed with researchers at Dartmouth College, including work related to the Data Hemorrhages article, in which the 1718 File is excerpted (CX0382). *See, e.g.*, CX0703 at 134; RX541 at 56. During the November 21, 2013 deposition of Tiversa’s Rule 3.33 designee, counsel did not develop any facts regarding Tiversa’s contracts with government agencies. CX703. Respondent’s counsel, Cause of Action, did, however, submit to the Commission a May 3, 2013 FOIA request for, *inter alia*, all contracts between Tiversa and the Commission (**Ex. G**), of which there are none. *See* RX541 at 98. In response to an unanticipated question during Complaint Counsel’s May 20, 2014 opening statement, Complaint Counsel mistakenly stated that Tiversa had received no federal funding. *Compare* Resp. Mot. at 6 *with* RX541 at 14 (June 7, 2014 testimony).

at multiple Internet Protocol (“IP”) addresses.⁷ That the 1718 File was found on a P2P network at multiple IP addresses only amplifies the likely injury.

Respondent has offered *no* admissible evidence to support its bald allegation that Tiversa “stole the 1718 File.” Mot. at 4 n.3. Assuming, counterfactually, that there were evidence of Tiversa having downloaded the 1718 File from a computer used by LabMD’s billing manager, the 1718 File’s presence on a P2P network would remain a cognizable injury, if for no other reason than that others had access to it. *See* Order Den. Mot. for Sum. Decision (May 19, 2014) at 6-7 (“MSD Order”) (“[E]ven if we accepted as true the claim[] that Tiversa retrieved the Insurance Aging File without LabMD’s knowledge or consent . . . , [it] would not compel us, as a matter of law, to dismiss the allegations in the Complaint that LabMD failed to implement reasonable and appropriate data security To the contrary, LabMD’s factual contentions concerning Tiversa . . . are fully consistent with the Complaint’s allegations that LabMD failed to implement reasonable and appropriate data security procedures.”). Georgia statutory law, which no court has applied to P2P, does not change this analysis. *See, e.g., Loud Records LLC v. Minervini*, 621 F. Supp. 2d 672, 678 (W.D. Wisc. 2009) (interpreting the analogous federal statute, 18 U.S.C. § 1030(a), concluding that “because the [P2P] files that plaintiffs allegedly accessed were *accessible by the public*, any allegation . . . that plaintiffs acted without authorization is tenuous at best”) (emphasis added); *accord Motown Record Co. L.P. v. Kovalcik*, 2009 WL 455137, at *3 (E.D. Pa. 2009); *see also U.S. v. Mullin*, 178 F.3d 334, 340 n.1 (5th Cir.

⁷ *See, e.g.,* CX0703 (Boback testimony) at 111; RX541 (Boback testimony) at 76. *Cf.* RX541 at 67 (no knowledge of Tiversa having downloaded the 1718 File from a workstation at LabMD). Contrary to Respondent’s assertion, Mot. at 3, there is no evidence in the record that Mr. Boback’s testimony “that the 1718 File was ‘found’ at various IP addresses specified in CX-19” is “a lie.”

1999) (citing *Burdeau v. McDowell*, 256 U.S. 465 (1921), to conclude that “the Fourth Amendment does not require suppression of evidence taken illegally by private citizens”).

III. RESPONDENT’S MOTION IGNORES SUBSTANTIAL EVIDENCE OF LABMD’S UNLAWFUL DATA SECURITY PRACTICES

Separate from the 1718 File, the evidentiary record contains significant evidence of LabMD’s failure to reasonably and appropriately protect consumers’ personal information on its computer networks. *Cf.* MSD Order at 9 (identifying as one of the “central questions” whether “LabMD’s data security practices were reasonable”). Specifically, the evidentiary record establishes that LabMD failed to: (1) develop, implement, or maintain a comprehensive data security program;⁸ (2) use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities;⁹ (3) use adequate measures to prevent employees from accessing consumers’ personal information not needed to perform their jobs;¹⁰ (4) adequately train employees on basic security practices;¹¹ (5) require employees and others to use common authentication-related security measures;¹² (6) maintain and update operating systems on computers and other devices;¹³ and (7) use readily available measure to prevent and detect unauthorized access to consumers’ personal information.¹⁴ Compl. ¶ 10. As such, Respondent has grossly mischaracterized Complaint Counsel’s evidence of LabMD’s unlawful data security practices.

⁸ *See, e.g.*, Trial Tr. at 125-36; JX0001, Facts 6-7.

⁹ *See, e.g.*, Trial Tr. at 137-63; JX0001, Fact 8; CX0035; CX0070.

¹⁰ *See, e.g.*, Trial Tr. at 163-67; JX0001, Fact 5; CX0754.

¹¹ *See, e.g.*, Trial Tr. at 167-76.

¹² *See, e.g.*, Trial Tr. at 176-88; CX0167.

¹³ *See, e.g.*, Trial Tr. at 188-94; CX0067; CX0051.

¹⁴ *See, e.g.*, Trial Tr. at 194-202.

CONCLUSION

For the foregoing reasons, the Court should deny Respondent's Motion for Sanctions.

Dated: August 25, 2014

Respectfully submitted,



Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown

Federal Trade Commission
600 Pennsylvania Ave., NW
Room CC-8232
Washington, DC 20580
Telephone: (202) 326-3321 - Sheer
Facsimile: (202) 326-3393
Electronic mail: asheer@ftc.gov

Complaint Counsel

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

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

[PROPOSED] ORDER DENYING RESPONDENT’S MOTION FOR SANCTIONS

Upon consideration of Respondent’s Motion for Sanctions and Complaint Counsel’s Opposition thereto, it is hereby ORDERED that Respondent’s Motion is DENIED.

ORDERED:

D. Michael Chappell
Chief Administrative Law Judge

Date:

CERTIFICATE OF SERVICE

I hereby certify that on August 25, 2014, I caused the foregoing document to be filed electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

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

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

I further certify that I caused a copy of the foregoing document to be served *via* electronic mail to:

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

Reed Rubinstein
William A. Sherman, II

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

CERTIFICATE FOR ELECTRONIC FILING

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

August 25, 2014

By:

A handwritten signature in black ink, appearing to read 'Jarad Brown', is written over a solid horizontal line.

Jarad Brown
Federal Trade Commission
Bureau of Consumer Protection

Exhibit A

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

COMPLAINT COUNSEL’S INITIAL DISCLOSURES

Pursuant to Rule 3.31(b) of the Federal Trade Commission’s Rules of Practice, 16 C.F.R. § 3.31(b), Complaint Counsel hereby serves its Initial Disclosures on Respondent LabMD, Inc. (“LabMD” or “Respondent”). The information disclosed herein is based upon information reasonably available to Complaint Counsel. Without waiving any privileges or prejudicing the ability to supplement these Initial Disclosures if additional information becomes available, Complaint Counsel makes the following disclosures:

I. Individuals Likely to Have Discoverable Information

Pursuant to Rule 3.31(b)(1), Complaint Counsel identifies the individuals listed in **Appendix A** as those who are likely to have discoverable information relevant to the allegations asserted in the Complaint, the proposed relief, or the defenses of Respondent. Complaint Counsel has set forth each individual’s name and the last known address and telephone number.¹ Because **Appendix A** contains information drawn from documents produced in the

¹ If an entity is likely to have discoverable and relevant information, but Complaint Counsel does not know the name of an individual associated with that entity who is likely to have such information, Complaint Counsel has provided the name of the entity and the last known address and telephone number.

Commission's investigation of Respondent, Complaint Counsel has marked **Appendix A** as confidential, pursuant to the Protective Order entered in this matter on August 29, 2013.

Respondent presently knows the identities of its current and former employees, clients, contractors, and other service and equipment providers, and any other individuals who have performed work for LabMD, with or without pay, all of whom may have discoverable and relevant information. **Appendix A** identifies the current and former LabMD employees, clients, contractors, and other service and equipment providers, who, based on Complaint Counsel's present knowledge, are likely to have discoverable and relevant information.

Pursuant to Rule 3.31A, Complaint Counsel will disclose the identity of testifying expert(s), if any, at a later date in compliance with the Scheduling Order to be entered in this matter.

II. Relevant Documents and Electronically Stored Information

Pursuant to Rule 3.31(b)(2), Complaint Counsel is producing to Respondent on the enclosed encrypted disc copies of "all documents," "electronically stored information," and "tangible things" ("Documents") in the "possession, custody, or control of the Commission" that are "relevant to the allegations of the Commission's complaint, to the proposed relief, or to the defenses of the respondent," and are not:

1. Subject to the limitations in Rule 3.31(c)(2);
2. Privileged as defined in Rule 3.31(c)(4);
3. Pertaining to hearing preparation as defined in Rule 3.31(c)(5);
4. Pertaining to experts as defined in Rule 3.31A; or
5. Obtainable from another source that is "more convenient, less burdensome, or less expensive."

The documents that Complaint Counsel is producing to Respondent as part of these Initial Disclosures are as labeled as follows:

- FTC-000001 – FTC-000893;
- FTC-SAC-000001 – FTC-SAC-000044; and
- FTC-PRI-000001 – FTC-PRI-001724.

The documents labeled FTC-SAC-000001 – FTC-SAC-000044 were provided to the Commission by the Sacramento, California Police Department voluntarily *in lieu* of compulsory process. The documents labeled FTC-PRI-000001 – FTC-PRI-001724 were provided to the Commission by the Privacy Institute pursuant to compulsory process.

Complaint Counsel is without knowledge at this time as to the category and location of relevant documents in the possession, custody, or control of Respondent. Complaint Counsel believes that Respondent generally is in the possession of documents relevant to the allegations of the Commission's complaint, and anticipates that Respondent will provide this information as part of its mandatory initial disclosures.

Dated: September 24, 2013

Respectfully submitted,

/s/ Margaret L. Lassack
Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm

Complaint Counsel
Federal Trade Commission
600 Pennsylvania Avenue NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-3321 - (Sheer)
Facsimile: (202) 326-3062
Electronic mail: asheer@ftc.gov

CERTIFICATE OF SERVICE

This is to certify that on September 24, 2013, I caused Complaint Counsel's Initial

Disclosures to be served *via* hand delivery and electronic mail on:

Michael D. Pepson
Regulatory Counsel
Cause of Action
1919 Pennsylvania Avenue NW, Suite 650
Washington, DC 20006
michael.pepson@causeofaction.org

Reed Rubinstein
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue NW
Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com

Counsel for Respondent LabMD, Inc.

September 24, 2013

By: /s/ Margaret L. Lassack
Margaret Lassack
Federal Trade Commission
Bureau of Consumer Protection

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Exhibit B

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

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

COMPLAINT COUNSEL’S PRELIMINARY WITNESS LIST

Pursuant to the Court’s Revised Scheduling Order, dated October 22, 2013, Complaint Counsel hereby provides its Preliminary Witness List to Respondent LabMD, Inc. (“LabMD” or “Respondent”). This list identifies the fact witnesses who may testify for Complaint Counsel at the hearing in this action by deposition and/or investigational hearing transcript, declaration, or orally by live witness. It does not identify expert or rebuttal expert witnesses, whom Complaint Counsel will identify at a later date in compliance with the Scheduling Order and Revised Scheduling Order entered in this action.

The information disclosed herein is based upon information reasonably available to Complaint Counsel at present. Discovery is ongoing and likely will have an impact on Complaint Counsel’s final proposed witness list. Subject to the limitations in the Scheduling Order and Revised Scheduling Order entered in this action, Complaint Counsel reserves the right:

- A. To present testimony by deposition and/or investigational hearing transcript, declaration, or orally by live witness, from any other person that Respondent identifies as a potential witness in this action;

- B. For any individual listed below as being associated with a corporation, government agency, or other non-party entity, to substitute a witness designated by the associated non-party entity in response to any subpoena that has been or may be issued by Complaint Counsel or Respondent to that non-party entity in this action;
- C. To present testimony by deposition and/or investigational hearing transcript, declaration, or orally by live witness, from the custodian of records of any non-party from which documents or records have been or will be obtained in this action, including, but not limited to, the non-parties listed below, to the extent necessary for the admission of documents or deposition or investigational hearing testimony into evidence in the event that a stipulation cannot be reached concerning the admissibility of such documents or testimony;
- D. To present testimony by deposition and/or investigational hearing transcript, declaration, or orally by live witness, from any witnesses to rebut the testimony of witnesses proffered by Respondent;
- E. Not to present testimony by deposition and/or investigational hearing transcript, declaration, or orally by live witness, from any of the witnesses listed below; and
- F. To supplement this Preliminary Witness List if additional information becomes available through discovery or otherwise.

Subject to these reservations of rights, Complaint Counsel's preliminary list of witnesses is as follows:

Current and Former LabMD Employees

1. John Boyle, former LabMD Vice President of Operations

We expect that Mr. Boyle will testify both in his individual capacity and as LabMD's corporate designee during the Part II investigation. We expect that he will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's

security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's expenditures related to information technology ("IT"); management of LabMD's compliance program; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

2. Brandon Bradley, former LabMD IT employee

We expect that Mr. Bradley will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

3. Sandra Brown, former LabMD finance or billing employee

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

4. Matt Bureau, former LabMD IT employee

We expect that Mr. Bureau will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

5. Michael Daugherty, LabMD President and Chief Executive Officer

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

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

We expect that Mr. Dooley will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

7. Liz Fair, former LabMD finance or billing employee

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

8. Karalyn Garrett, former LabMD finance or billing employee

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

9. Patricia Gilbreth, LabMD finance or billing employee

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

10. Patrick Howard, former LabMD IT employee

We expect that Mr. Howard will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

11. Lawrence Hudson, former LabMD sales employee

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

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

We expect that Mr. Hyer will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

13. Curt Kaloustian, former LabMD IT employee

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

14. Eric Knox, former LabMD sales employee

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

15. Chris Maire, former LabMD IT employee

We expect that Mr. Maire will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

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

We expect that Mr. Martin will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which he and other LabMD employees had access; LabMD's IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

17. Jennifer Parr, LabMD IT employee

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

18. Alison Simmons, former LabMD IT employee

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

19. Connie Wavrin, former LabMD Lab Manager and Safety Coordinator

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

20. Rosalind Woodson, former LabMD finance or billing employee

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

21. LabMD – designated witness(es) to be determined

We expect that one or more witnesses designated by LabMD will testify about LabMD’s computer networks, including, but not limited to, remote access thereto; LabMD’s security policies and practices, and employee training; the personal information to which LabMD employees had access; LabMD’s IT-related expenditures; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents. We also expect that LabMD will testify about any other topics listed in any deposition notice that may be issued by Complaint Counsel to LabMD in his action.

Current and Former Clients of LabMD

22. Midtown Urology, PC (“Midtown Urology”) – designated witness(es) to be determined

We expect that one or more witnesses designated by Midtown Urology will testify about Midtown Urology’s relationship and communications with LabMD; computer hardware and software provided to Midtown Urology by LabMD, and the maintenance thereof; and the transmission of personal information between Midtown Urology and LabMD. We also expect that the witness(es) designated by Midtown Urology will testify about facts relating to the documents produced in response to Complaint Counsel’s subpoena *duces tecum* to Midtown Urology in this action, and the admissibility of those documents into evidence in the hearing in this action.

23. Southeast Urology Network (“S.U.N.”) – designated witness(es) to be determined

We expect that one or more witnesses designated by S.U.N. will testify about S.U.N.’s relationship and communications with LabMD; computer hardware and software provided to S.U.N. by LabMD, and the maintenance thereof; and the transmission of personal information between S.U.N. and LabMD. We also expect that the witness(es)

designated by S.U.N. will testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to S.U.N. in this action, and the admissibility of those documents into evidence in the hearing in this action.

24. 21st Century Oncology, LLC d/b/a UroSurg Associates ("UroSurg") – designated witness(es) to be determined

We expect that one or more witnesses designated by UroSurg will testify about UroSurg's relationship and communications with LabMD; computer hardware and software provided to UroSurg by LabMD, and the maintenance thereof; and the transmission of personal information between UroSurg and LabMD. We also expect that the witness(es) designated by UroSurg will testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to UroSurg in this action, and the admissibility of those documents into evidence in the hearing in this action.

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

25. Brian Bissel, former LabMD contractor

We expect that Mr. Bissel will testify about LabMD's computer networks, including, but not limited to, remote access thereto; the products and/or services that he provided to LabMD, including but not limited to the security features of those products and/or services; LabMD's security policies and practices; the personal information to which he and LabMD employees had access; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

26. Hamish Davidson, President of ProviDyn, Inc.

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

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

We expect that Mr. Truett will testify about LabMD's computer networks, including, but not limited to, remote access thereto; the products and/or services that he and his company, Automated PC Technologies, Inc., provided to LabMD, including but not limited to the security features of those products and/or services; the communications between LabMD and Mr. Truett or Automated PC Technologies, Inc.; and the facts underlying and set forth in the affidavit that Mr. Truett executed on May 20, 2011, which LabMD submitted to Commission staff during the Part II investigation.

28. Cypress Communications, LLC ("Cypress") – designated witness(es) to be determined

We expect that one or more witnesses designated by Cypress will testify about LabMD's computer networks, including, but not limited to, remote access thereto; and the products and/or services that Cypress has provided to LabMD, including but not limited to any security features of those products and/or services. We also expect that the witness(es) designated by Cypress will testify about facts relating to the documents produced in response to Complaint Counsel's subpoena *duces tecum* to Cypress in this action and the admissibility of those documents into evidence in the hearing in this action.

Other Individuals and Entities

29. Robert Boback, Chief Executive Officer of Tiversa Holding Corporation (“Tiversa”)

We expect that Mr. Boback will testify, as Tiversa’s corporate designee, about Tiversa’s understanding and use of peer-to-peer file sharing applications and networks; Tiversa’s communications with LabMD; facts relating to how Tiversa obtained multiple copies of the “P2P insurance aging file” referenced in Paragraph 17 of the Complaint and the different IP addresses from which Tiversa obtained copies of that file; and other facts relating to the security incident alleged in Paragraphs 17-20 of the Complaint. We also expect that Mr. Boback will testify about facts relating to the documents produced in response to Complaint Counsel’s subpoena *duces tecum* to Tiversa Holding Corporation in this action and the admissibility of those documents into evidence in the hearing in this action.

30. Erick Garcia

We expect that Mr. Garcia will testify about the conduct underlying his plea of no contest to California charges of identity theft entered on March 6, 2013 in the Superior Court of California, County of Sacramento, and other facts relating to the security incident alleged in Paragraph 21 of the Complaint.

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

We expect that Detective Jestes will testify about facts relating to the security incident alleged in Paragraph 21 of the Complaint, including but not limited to, facts relating to her investigation of the conduct underlying the pleas of no contest to California charges of identity theft entered by Erick Garcia and Josie Martinez Maldonado, and her training and experience as it relates to identity theft. We also expect that Detective Jestes will testify about facts relating to the documents produced in response to Complaint Counsel’s subpoena

duces tecum to the Custodian of Records of the Sacramento, CA Police Department in this action and the admissibility of those documents into evidence in the hearing in this action.

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

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

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

We expect that Detective Lapidés will testify about his communications with LabMD and other facts relating to the security incident alleged in Paragraph 21 of the Complaint. We also expect that Detective Lapidés will testify about facts relating to any documents that may be produced in response to Complaint Counsel's subpoena *duces tecum* to the Sandy Springs, GA Police Department in this action, and the admissibility of those documents into evidence in the hearing in this action.

34. Josie Martinez Maldonado

We expect that Ms. Maldonado will testify about the conduct underlying her plea of no contest to California charges of identity theft entered on March 27, 2013 in the Superior Court of California, County of Sacramento, and other facts relating to the security incident alleged in Paragraph 21 of the Complaint.

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

We expect that Ms. McAndrew will testify about the existence or non-existence of any evaluations by HHS of LabMD's compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic

and Clinical Health Act (“HITECH”), and the regulations promulgated under HIPAA and HITECH.

36. Scott Moulton, President of and Lead Certified Computer Forensic Specialist for Forensic Strategy Services, LLC

We expect that Mr. Moulton will testify about the facts underlying and set forth in the affidavit that he executed on January 12, 2012, which LabMD filed in support of its response to the motion to dismiss filed by Tiversa in *LabMD, Inc. v. Tiversa, Inc.*, No. 11-cv-04044 (N.D. Ga. Jan. 13, 2012).

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

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

38. Andrew Craig Troutman, Associate General Counsel of Elavon, Inc., a wholly owned subsidiary of U.S. Bank National Association

We expect that Mr. Troutman will testify about facts related to the admissibility of documents produced by Elavon, Inc. in response to Complaint Counsel’s subpoena *duces tecum* to U.S. Bank National Association, ND into evidence in the hearing in this action.

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

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

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

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

Dated: December 19, 2013

Respectfully submitted,

/s/ Margaret L. Lassack

Alain Sheer

Laura Riposo VanDruff

Megan Cox

Margaret Lassack

Ryan Mehm

John Krebs

Complaint Counsel

Federal Trade Commission

600 Pennsylvania Avenue NW

Room NJ-8100

Washington, DC 20580

Telephone: (202) 326-3713 - (Lassack)

Facsimile: (202) 326-3062

Electronic mail: mlassack@ftc.gov

CERTIFICATE OF SERVICE

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

Michael D. Pepson
Lorinda Harris
Hallee Morgan
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
michael.pepson@causeofaction.org
lorinda.harris@causeofaction.org
hallee.morgan@causeofaction.org

Reed Rubinstein
William Sherman, II
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com
william.sherman@dinsmore.com

Counsel for Respondent LabMD, Inc.

December 19, 2013

By: /s/ Margaret L. Lassack
Margaret Lassack
Federal Trade Commission
Bureau of Consumer Protection

Exhibit C

2. Kim Gardner, former LabMD Executive Assistant

We expect that Ms. Gardner will testify about LabMD's computer networks, including, but not limited to, remote access thereto; LabMD's security policies and practices, and employee training; the personal information to which she and other LabMD employees had access; information relating to the wind down of LabMD's business operations and the corresponding relocation of LabMD's business premises; and facts relating to the security incidents alleged in Paragraphs 17-21 of the Complaint or any other security incidents.

3. Nicotra Harris, former LabMD finance or billing employee

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

4. Lou Carmichael, former LabMD consultant

We expect Ms. Carmichael will testify about LabMD's security policies and practices, compliance program, and employee training.

5. Jonn Perez, Trend Micro Inc. employee

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

6. Matt Wells, Trend Micro Inc. employee

We expect Mr. Wells will testify about facts related to the admissibility of documents that may be produced in response to Complaint Counsel’s subpoena *duces tecum* to Trend Micro Inc.

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

We expect Dean Johnson will testify about facts related to his study entitled “Data Hemorrhages in the Health-Care Sector,” including his research methodology and findings, the “P2P insurance aging file” referenced in Paragraph 17 of the Complaint, facts relating to the security incident alleged in Paragraphs 17-20 of the Complaint, peer-to-peer file sharing applications and networks, and the consequences of inadvertent disclosures of consumers’ personal information.

Complaint Counsel continues to reserve all rights reserved in its Preliminary Witness
List served to Respondent on December 19, 2013.

Dated: February 27, 2014

Respectfully submitted,

/s/ Margaret L. Lassack

Alain Sheer

Laura Riposo VanDruff

Megan Cox

Margaret Lassack

Ryan Mehm

John Krebs

Jarad Brown

Complaint Counsel

Federal Trade Commission

600 Pennsylvania Avenue NW

Room NJ-8100

Washington, DC 20580

Telephone: (202) 326-3713 - (Lassack)

Facsimile: (202) 326-3062

Electronic mail: mlassack@ftc.gov

CERTIFICATE OF SERVICE

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

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

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

Counsel for Respondent LabMD, Inc.

February 27, 2014

By: /s/ Megan Cox
Megan Cox
Federal Trade Commission
Bureau of Consumer Protection

Exhibit D

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

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

COMPLAINT COUNSEL’S FINAL PROPOSED WITNESS LIST

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

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

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

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

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

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

Current and Former LabMD Employees

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

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

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

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

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

3. Brandon Bradley, former LabMD IT employee

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

4. Sandra Brown, former LabMD finance or billing employee

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

5. Matt Bureau, former LabMD IT employee

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

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

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

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

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

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

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

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

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

9. Kim Gardner, former LabMD Executive Assistant

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

10. Karalyn Garrett, former LabMD finance or billing employee

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

11. Patricia Gilbreth, former LabMD finance or billing employee

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

12. Nicotra Harris, former LabMD finance or billing employee

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

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

13. Patrick Howard, former LabMD IT employee

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

14. Lawrence Hudson, former LabMD sales employee

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

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

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

16. Curt Kaloustian, former LabMD IT employee

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

17. Eric Knox, former LabMD sales employee

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

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

18. Chris Maire, former LabMD IT employee

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

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

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

20. Jennifer Parr, former LabMD IT employee

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

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

21. Alison Simmons, former LabMD IT employee

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

22. LabMD, designee(s) to be determined

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

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

Current and Former Clients of LabMD

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

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

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

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

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

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

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

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

26. Lou Carmichael, former LabMD consultant

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

27. Hamish Davidson, President of ProviDyn, Inc.

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

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

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

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

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

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

Other Individuals and Entities

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

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

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

31. Erick Garcia

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

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

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

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

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

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

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

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

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

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

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

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

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

37. Jonn Perez, Trend Micro Inc. employee

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

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

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

39. Matt Wells, Trend Micro Inc. employee

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

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

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

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

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

Expert Witnesses

42. Raquel Hill, PhD

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

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

network and (2) could have corrected any such security failures at relatively low cost using readily available security measures. Her testimony is based on transcripts and exhibits from investigational hearings and depositions of Respondent, its current and former employees, and third parties; correspondence and documents submitted by Respondent and third parties in connection with the pre-complaint investigation or this litigation; and industry and government standards, guidelines, and vulnerability databases that establish best practices for information security practitioners.

43. Rick Kam, CIPP/US

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

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

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


44. James Van Dyke

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

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

Dated: March 26, 2014

Respectfully submitted,



Alain Sheer

Laura Riposo VanDruff

Megan Cox

Margaret Lassack

Ryan Mehm

John Krebs

Jarad Brown

Complaint Counsel

Federal Trade Commission

600 Pennsylvania Avenue NW

Room NJ-8100

Washington, DC 20580

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

Facsimile: (202) 326-3062

Electronic mail: mcox1@ftc.gov

CERTIFICATE OF SERVICE

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

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

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

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

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

March 26, 2014


By: 
Megan Cox
Federal Trade Commission
Bureau of Consumer Protection

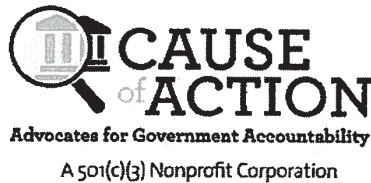
Exhibit E

CONFIDENTIAL – REDACTED IN ENTIRETY

Exhibit F

CONFIDENTIAL – REDACTED IN ENTIRETY

Exhibit G



May 3, 2013

VIA E-MAIL AND CERTIFIED MAIL

FOIA-2013-00848

David C. Shonka
Acting General Counsel
Office of General Counsel
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
E-mail: FOIA@ftc.gov

FEDERAL TRADE COMMISSION
RECEIVED

MAY 06 2013

FOIA BRANCH
GENERAL COUNSEL

RE: Freedom of Information Act Request

Dear Mr. Shonka

We write on behalf of Cause of Action, a non-profit, nonpartisan government accountability organization that fights to protect economic opportunity when federal regulations, spending and cronyism threaten it.

Under section 5 of the Federal Trade Commission Act (FTCA), Congress authorized the Federal Trade Commission (FTC) to investigate, via civil investigative demands (CIDs), unfair or deceptive acts or practices that affect commerce.¹ Consistent with this authority, the FTC may issue resolutions "authorizing the use of compulsory process" when the public interest demands it.² On January 3, 2008, the FTC issued a resolution authorizing civil investigations of entities believed to have engaged in unfair or deceptive practices that affect consumer privacy or data security.³

On February 5, 2008, Tiversa, Incorporated (Tiversa),⁴ a for-profit,⁵ federally-funded⁶ company obtained business-related records, including records containing personal health

¹ 15 U.S.C. § 57b-1. See 15 U.S.C. §§ 45, 49, 50.

² 16 C.F.R. § 2.7(a).

³ FED. TRADE COMM'N, RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY AND/OR DATA SECURITY (Jan. 3, 2008) (FTC File No. P954807) (on file with author).

⁴ Tiversa, Inc., a Pennsylvania Corporation, is also registered with the Pennsylvania Department of State as Tiversa Entertainment Group, Tiversa Government, Incorporated, Tiversa Holding Corporation, Tiversa IP, Inc., Tiversa Labs, Tiversa Media, Inc. and Tiversa Real Estate Holdings, LLC (collectively, "Tiversa Entities").

⁵ This project was in conjunction with Dartmouth College and was funded by DHS and DOJ grants. See *Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand*, FTC File No. 102 3099, at 2 (Jan. 10, 2012) available at <http://www.ftc.gov/os/quash/120110labmdmichaelpetition.pdf>.

⁶ This activity was partially supported by the U.S. Department of Homeland Security under Grant Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P).

1919 Pennsylvania Ave, NW
Suite 650
Washington, DC 20006

www.CauseOfAction.org

Ph: 202.499.4232

Mr. David C. Shonka
May 3, 2013
Page 2

information (PHI) from LabMD, a private medical testing company. Tiversa obtained these records without LabMD's knowledge or consent and subsequently turned them over to the FTC after LabMD refused to engage Tiversa's electronic security services.

On December 21, 2011, the FTC issued a CID to LabMD⁷ and another to its President, Michael J. Daugherty.⁸ In these CIDs, the FTC requested certain documents.⁹ LabMD filed a motion to quash the CIDs but the motion was denied by the FTC, with one commissioner dissenting. In his dissent, FTC Commissioner J. Thomas Rosch expressed concern "that Tiversa is more than an ordinary witness, informant, or 'whistle-blower' in this matter because it is a commercial entity with 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."¹⁰ Nonetheless, the FTC took the position that LabMD's data security practices may have violated section 5 of the FTCA.

Cause of Action seeks to understand how the FTC conducts its investigations and recommendations for CIDs, analyzes legal issues that arise in conducting a CID, and ensures the protection of entities under investigation. Therefore, pursuant to the Freedom of Information Act (FOIA),¹¹ Cause of Action requests that the FTC produce, within the next twenty (20) business days, the following documents, from the time period of January 3, 2008 to the present:

1. All records, including guidance memoranda and policy documents, referring or relating to the FTC's obligations under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,¹²
2. All records, including guidance memoranda and policy documents, referring or relating to the FTC's authority to issue CIDs;
3. All records, including guidance memoranda and policy documents, referring or relating to the FTC's standards for conducting consumer privacy or data security investigations through the CID process;
4. All documents, including e-mail communications, used by, regarding, referring or relating to CIDs conducted by the FTC under the authority of the 2008 *Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security*,¹³
5. All records, including e-mail communications, between employees or officers of the FTC and third-party informants, including but not limited to the Tiversa Entities, Dartmouth

⁷ FED. TRADE COMM'N, Civil Investigative Demand to LabMD, FTC Form 144 (Dec. 21, 2011) [hereinafter LabMD CID]

⁸ FED. TRADE COMM'N, Civil Investigative Demand to Michael J. Daugherty, President, LabMD, FTC Form 144 (Dec. 21, 2011) [hereinafter Daugherty CID]

⁹ LabMD CID; Daugherty CID.

¹⁰ *Petitions of LabMD, Inc & Michael J. Daugherty to Limit or Quash the Civil Investigative Demands*, (Comm'r J. Thomas Rosch, dissenting) FTC File No. 1023099, at 1 (June 21, 2012).

¹¹ 5 U.S.C. § 552 (2006 & Supp. II 2008).

¹² Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

¹³ FEDERAL TRADE COMMISSION, RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY AND/OR DATA SECURITY (Jan. 3, 2008) (FTC File No. P954807) (on file with author)

- College and/or I3P, that refer or relate to entities the FTC investigates under its CID authority;
6. All records, including e-mail communications, referring or relating to any third-party informant, including but not limited to the Tiversa Entities or Dartmouth College, that mention the third party informant's receipt of federal funds or its status as a federally funded entity; and
 7. All contracts, grants or funding requisitions between the FTC and the Tiversa Entities, Dartmouth College and/or the I3P.

For those records for which the FTC is claiming privilege, please indicate the date range for which the privilege applies. If any communications exist before privilege arises, please produce those records in their entirety.

Cause of Action Is Entitled to a Complete Waiver of Fees (Public-Interest Purpose).

Cause of Action requests a waiver of both search and review fees pursuant to 5 U.S.C. § 552(a)(4)(A)(iii). This statute provides that the requested information and/or documents shall be furnished without or at reduced charge if "disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." Cause of Action, in the present matter, satisfies all of the required elements for a fee waiver.

- A. *Disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government.*

First and foremost, "obtaining information to act as a 'watchdog' of the government is a well-recognized public interest in the FOIA."¹⁴ It is for this reason that Cause of Action, a nonprofit, nonpartisan organization that uses investigative, legal and communications tools to educate the public on how government accountability and transparency protects taxpayer interests and economic opportunity, seeks disclosure of the requested documents. Disclosure of the information requested by Cause of Action in this instance is likely to contribute significantly to the understanding by the public at large of the operations and activities of the federal government as all the documents requested concern how the FTC conducts the CID process, including its procedures for ensuring evidence is properly acquired and its relationships with third-party informants.

The public at large has a moral and financial interest in knowing whether the FTC has acted fairly in investigating purported allegations of unfair or deceptive trade practices. Because of this, the information requested will benefit the public as opposed to the individual understanding of the requester or a narrow segment of interested persons. Disclosure would undoubtedly be of value to members of the public. Thus, this element is met.

¹⁴ *Balt. Sun v. U.S. Marshals Serv.*, 131 F. Supp. 2d 725, 729 (D. Md. 2001); *see also* *Ctr. to Prevent Handgun Violence v. U.S. Dep't of the Treasury*, 981 F. Supp. 20, 24 (D.D.C. 1997) ("This self-appointed watchdog role is recognized in our system").

B. Disclosure of the requested information is not in the commercial interest of Cause of Action.

Cause of Action does not seek this information to benefit commercially. Cause of Action is a non-profit organization as defined under § 501(c)(3) of the Internal Revenue Code. Our organization is committed to protecting the public's right to be aware of the activities of government agencies and to ensuring the lawful and appropriate use of government funds by those agencies. This request covers the manner in which the FTC conducts civil investigations of alleged unfair or deceptive trade practices. Cause of Action will not make a profit from the disclosure of this information. This information will be used to further the knowledge and interests of the general public regarding the FTC's operations while providing an opportunity for the public to evaluate the FTC's performance in relation to alleged misconduct by Tiversa and LabMD. In the event the disclosure of this information creates a profit motive, it is not dispositive for the commercial interest test; media or scholars could have a profit motive, as long as the dissemination of the information is in their professional capacity and would further the public interest.¹⁵ Therefore, Cause of Action satisfies this element.

C. Cause of Action has an ability to disseminate the requested information to the public and specifically intends to do so.

Cause of Action intends to make the results of this request available to the public in various medium forms. Cause of Action uses a combination of research, litigation, advocacy and regularly disseminated publications to advance its mission. Our staff has a combined forty-five (45) years of expertise in government oversight, investigative reporting and federal public interest litigation. These professionals will analyze the information responsive to this request, use their editorial skills to turn raw materials into a distinct work and share the resulting analysis with the public, whether through Cause of Action's regularly published online newsletter, memoranda, reports or press releases. In addition, Cause of Action will disseminate any relevant information it acquires from this request to the public through its frequently visited website, www.causeofaction.org, which also includes links to thousands of pages of documents Cause of Action acquired through its previous FOIA requests, as well as documents related to Cause of Action's litigation and agency complaints. Lastly, after the production of the requested information, Cause of Action intends to produce a report on the matter of any prohibited or unethical conduct at the FTC. This report may be published, distributed to the news media and sent to interested persons through our regular periodicals, including "Agency Check" and "Cause of Action News." An ability to show the presence of a website with occasional, consistent traffic is enough to show that a requester has an ability to disseminate information.¹⁶ As with the other two (2) outlined above, Cause of Action has also met this element, thus justifying a fee waiver.

¹⁵ See *Campbell v. U.S. Dep't of Justice*, 164 F.3d 20, 38 (D.C. Cir. 1998).

¹⁶ See *FedCURE v. Lappin*, 602 F. Supp. 2d 197, 203 (D.D.C. 2009).

Cause of Action Is Entitled to News Media Requester Category Status.

Cause of Action also asks that it not be charged search or review fees for this request because it qualifies as a “representative of the news media, or news media requester,” under 5 U.S.C. § 552(a)(4)(A)(ii)(II).¹⁷ In *National Security Archive v. U.S. Dep’t of Defense*,¹⁸ the U.S. Court of Appeals for the District of Columbia Circuit noted that FOIA’s legislative history demonstrates that “it is critical that the phrase ‘representative of the news media’ be broadly interpreted if the act is to work as expected . . . In fact, *any person or organization which regularly publishes or disseminates information to the public . . . should qualify for waivers as a ‘representative of the news media.’*”¹⁹

Cause of Action is organized and operated, *inter alia*, to publish and broadcast news, *i.e.*, information that is about current events or that would be of current interest to the public. Cause of Action routinely and systematically disseminates information to the public through various medium forms. Cause of Action maintains a frequently visited website, www.causeofaction.org. Additionally, since September 2011, Cause of Action has published an e-mail newsletter. This newsletter provides subscribers with regular updates regarding Cause of Action’s activities and information the organization has received from various government entities. Cause of Action also disseminates information via Twitter and Facebook. Cause of Action also produces a newsletter titled “Agency Check,” which informs interested persons about actions of federal agencies, and another periodical, “Cause of Action News.”²⁰

Cause of Action gleans the information it regularly publishes in its newsletters from a wide variety of sources, including FOIA requests, government agencies, universities, law reviews and even other news sources. Cause of Action researches issues on government transparency and accountability, the use of taxpayer funds and social and economic freedom; regularly reports on this information; analyzes relevant data; evaluates the newsworthiness of the material; and puts the facts and issues into context. Cause of Action uses technology, including but not limited to the Internet, Twitter and Facebook, in order to publish and distribute news about current events and issues that are of current interest to the general public. These activities are hallmarks of publishing, news and journalism. Based on these extensive publication activities, Cause of Action qualifies for a fee waiver as a “representative of the news media, or news media requester,” under FOIA and agency regulations.²¹

¹⁷ Other agencies of the federal government have granted Cause of Action “representative of the news media” category status. *See, e.g.*, FOIA Request HQ-2012-00752-F, Dep’t of Energy (Feb. 15, 2012); FOIA Request No. 12-00455-F, Dep’t of Educ. (Jan. 20, 2012); FOIA Request 12-267, Fed. Emergency Mgmt. Agency (Feb. 9, 2012); FOIA Request 2012-RMA-02563F, Dep’t of Agric. (May 3, 2012); FOIA Request 2012-078, Dep’t of Homeland Sec. (Feb. 15, 2012); FOIA Request 2012-00270, Dep’t of Interior (Feb. 17, 2012); FOIA Request, Dep’t of Labor (Apr. 20, 2012); FOIA Request CRRIF 2012-00077, Dep’t of Commerce (Mar. 1, 2012). As the U.S. Court of Appeals for the District of Columbia noted in *Oglesby v. U.S. Dep’t of the Army*, agencies should grant news media requester status when other agencies have done so because of “the need for uniformity among the agencies in their application of FOIA.” 920 F.2d 57, 66 (D.C. Cir. 1990).

¹⁸ 880 F.2d 1381, 1386 (D.C. Cir. 1989).

¹⁹ *Id.* (citing 132 Cong. Rec. S14298 (daily ed. Sept. 30, 1986)) (emphasis in original).

²⁰ Newsletters, Cause of Action, *available at* <http://causeofaction.org/newsletters/>.

²¹ *See, e.g.* Paul Streckfus, *Accountability Group Seeks IRS Investigation of ACORN Affiliates*, EO TAX JOURNAL, Ed. 2011-173, Oct. 24, 2011; Patrick Reis and Darren Goode, *Senators hedge bets ahead of CSAPR vote - Second*

Mr. David C. Shonka
May 3, 2013
Page 6

Cause of Action's activities clearly fall within the statutory definition of this term. 5 U.S.C. § 552(a)(4)(A)(ii)(III) defines "representative[s] of the news media" broadly to include organizations that disseminate news through electronic communications, including "*publishers of periodicals . . . who make their products available for purchase by or subscription by or free distribution to the general public.*"²² Moreover, the FOIA statute itself, as amended in 2007, explicitly defines "representative of the news media"—a term that had previously been undefined in the statute—to specifically include organizations, such as Cause of Action, that

anti-reg bill to get vote - Perry's debate gaffe - Acrimony hits new heights in Solyndra spat, POLITICO (Nov. 10, 2011), <http://www.politico.com/morningenergy/1111/morningenergy374.html>; Conn Carroll, *Labor board broke federal law on Boeing suit*, WASH. EXAMINER, Nov. 27, 2011, available at <http://campaign2012.washingtonexaminer.com/article/labor-board-broke-federal-law-boeing-suit>; Matthew Vadum, *Obama uses taxpayer cash to back ACORN Name changes used to dodge the law*, WASH. TIMES, Nov. 28, 2011, available at <http://www.washingtontimes.com/news/2011/nov/28/obama-uses-taxpayer-cash-to-back-acorn-name-change/>; Benjamin Wallace, *The Virgin Father*, N.Y. MAGAZINE (Feb. 5, 2012), available at <http://nymag.com/news/features/trent-arsenault-2012-2/>; Perry Chiaramonte, *ACORN Misused Federal Grant Funds, Report Says*, FOX NEWS (Nov. 30, 2011), <http://www.foxnews.com/politics/2011/11/30/acorn-misused-federal-grant-funds-report-says/>; Timothy R. Smith, *How much are other agencies spending on award coins? A nonpartisan group wants to know*, WASH. POST (Apr. 6, 2012), available at http://www.washingtonpost.com/blogs/federal-eye/post/how-much-are-other-agencies-spending-on-award-coins-a-nonpartisan-group-wants-to-know/2012/04/05/gIQAQlPpGPyS_blog.html; *Acorn lives: Meet AHCOA*, PITTSBURGH TRIBUNE-REVIEW, Dec. 5, 2011, available at http://www.pittsburghlive.com/x/pittsburghtrib/opinion/s_770135.html; Andy Medici, *Scrutiny widens over GSA spending*, FED. TIMES (Apr. 6, 2012), <http://www.federaltimes.com/article/20120406/DEPARTMENTS07/204060303/>; Charles C. W. Cooke, *ACORN Is Up to Its Old Tricks*, NAT'L REVIEW ONLINE (Feb. 6, 2012), <http://www.nationalreview.com/articles/289948/acorn-its-old-tricks-charles-c-w-cooke>; John Hayward, *Justice Department asked to investigate abuse of stimulus funds for lobbying*, HUMAN EVENTS (Mar. 3, 2012), <http://www.humanevents.com/article.php?id=50328>; Pete Kasperowicz, *GSA fallout: Watchdog group probes 28 federal agencies for wasteful spending*, THE HILL, Apr. 5, 2012, available at <http://thehill.com/blogs/floor-action/house/220119-gsa-fallout-watchdog-group-probes-28-federal-agencies-for-wasteful-spending>; Mickey Meece, *Durbin Calls GSA Spending 'Outrageous'; Vows Congressional Hearings*, FORBES.COM (Apr. 8, 2012), <http://www.forbes.com/sites/mickeymeece/2012/04/08/durbin-calls-gsa-spending-outrageous-vows-congressional-hearings/>; Christopher Matthews, *High Tide: From a Wal-Mart Feeding Frenzy to Indian Firms' Continued Shipping of Iranian Crude*, WALL ST. J., Apr. 24, 2012, available at <http://blogs.wsj.com/corruption-currents/2012/04/24/high-tide-from-a-wal-mart-feeding-frenzy-to-indian-firms-continued-shipping-of-iranian-crude/>; Lauren Fox, *Federal Budget Office Asks All Agencies to Cut Conference, Travel Costs*, US NEWS (May 12, 2012), <http://www.usnews.com/news/blogs/washington-whispers/2012/05/14/federal-budget-office-asks-all-agencies-to-cut-conference-travel-costs>; Stephanie Lee, *Woman sues FDA for right to use donor's free sperm*, S. F. CHRON., July 9, 2012, available at <http://www.sfgate.com/bayarea/article/Woman-sues-FDA-for-right-to-use-donor-s-free-sperm-3692207.php>; Alexis Shaw, *Woman Anonymously Sues FDA for Right to Free Sperm*, ABC NEWS (July 12, 2012), <http://abcnews.go.com/US/woman-sues-fda-free-sperm/story?id=16755422>; Perry Chiaramonte, *Taxpayer watchdog calls on IRS to probe re-branded Texas ACORN branch*, FOX NEWS (July 19, 2012), <http://www.foxnews.com/politics/2012/07/19/taxpayer-watchdog-calls-on-irs-to-probe-re-branded-texas-acorn-branch/#ixzz21qTFmosA>; Jon Hilkevitch, *Report: CTA reaped millions by over-reporting bus mileage*, CHI. TRIB. (Oct. 17, 2012), available at http://articles.chicagotribune.com/2012-10-18/news/ct-met-cta-mileage-report-1018-20121018_1_cta-spokesman-cta-officials-action-report; Nick Baumann, *National Archives Sued Over Financial Crisis Documents*, MOTHER JONES (Aug. 15, 2012), available at <http://www.motherjones.com/mojo/2012/08/watchdog-group-sues-national-archives-over-financial-crisis-documents>.

²² 5 U.S.C. § 552(a)(4)(A)(ii)(III) (emphasis added).

Mr. David C. Shonka
May 3, 2013
Page 7

regularly publish and disseminate online periodicals, *e.g.*, newsletters.²³ The statutory definition unequivocally commands that organizations that electronically disseminate information and publications via “alternative media *shall* be considered to be news-media entities.”²⁴ As the plain language of the statute makes abundantly clear, then, an organization that regularly disseminates news via an online newsletter or periodical, such as Cause of Action, is a “representative of the news media” under FOIA.

In *Electronic Privacy Information Center v. Dep’t of Defense*,²⁵ the court broadly construed a Department of Defense regulation defining “representative of the news media” to include a 501(c)(3) that, like Cause of Action, maintains a frequently visited website and regularly publishes an e-mail newsletter. Under well-established precedent, then, a 501(c)(3) requester that regularly publishes online newsletters, such as Cause of Action, is entitled to a fee waiver as a “representative of the news media,” where *Electronic Privacy Information Center* provides that “publishers of periodicals” qualify as representatives of the news media.²⁶

The information requested regarding the fairness of the FTC’s CIDs, its civil investigations and the means by which the FTC accumulates its evidence will be of current interest to a large segment of the general public. Cause of Action will ultimately disseminate this information that it is statutorily entitled to, *inter alia*, through its regularly published online newsletter. Additionally, Cause of Action will take the information that is disclosed, using its editorial skills and judgment, to publish news articles that will be published on our website, distributed to other media sources and distributed to interested persons through our newsletters.

As outlined above, the plain language of 5 U.S.C. § 552(a)(4)(A)(ii)(III), controlling precedent and the agency’s regulations clearly require the conclusion that Cause of Action is a representative of the news media.

²³ The FOIA statute, as amended in 2007, defines “representative of the news media” as follows:

[T]he term “a representative of the news media” means any person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience. In this clause, the term “news” means information that is about current events or that would be of current interest to the public. Examples of news-media entities are television or radio stations broadcasting to the public at large and publishers of periodicals (but only if such entities qualify as disseminators of “news”) who make their products available for purchase by or subscription by or free distribution to the general public. These examples are not all-inclusive. Moreover, as methods of news delivery evolve (for example, the adoption of the electronic dissemination of newspapers through telecommunications services), *such alternative media shall be considered to be news-media entities.*

5 U.S.C. § 552(a)(ii)(III) (emphasis added).

²⁴ *Id.* (emphasis added). See generally *Nat’l Ass’n of Home Builders v. Defenders of Wildlife*, 551 U.S. 644, 661-662 (2007) (noting the well-established proposition that, as used in statutes, the word “shall” is generally imperative or mandatory).

²⁵ 241 F.Supp.2d. 5, 12-15 (D.D.C. 2003). The court pointedly noted that “a ‘periodical,’ unlike a daily newspaper, has been defined simply as ‘a publication issued at regular intervals of more than one day.’” *Id.* at 14 n.4 (quoting *AMERICAN HERITAGE DICTIONARY, SECOND COLLEGE EDITION*, at 923 (2000)).

²⁶ *Elec. Privacy Info. Ctr v. Dep’t of Defense*, 241 F.Supp.2d. 5, 12-15 (D.D.C. 2003).

Mr. David C. Shonka
May 3, 2013
Page 8

Production of Information and Contact Information.

We call your attention to President Obama's January 21, 2009 Memorandum concerning FOIA, which states in relevant part:

All agencies should adopt a presumption in favor of disclosure, in order to renew their commitment to the principles embodied in FOIA . . . The presumption of disclosure should be applied to all decisions involving FOIA.²⁷

On the same day, President Obama spoke on FOIA to incoming members of the Cabinet and staff of the White House and stated in relevant part:

The old rules said that if there was a defensible argument for not disclosing something to the American people, then it should not be disclosed. That era is now over. Starting today, every agency and department should know that this administration stands on the side not of those who seek to withhold information but those who seek to make it known. To be sure, issues like personal privacy and national security must be treated with the care they demand. But the mere fact that you have the legal power to keep something secret does not mean you should always use it. The Freedom of Information Act is perhaps the most powerful instrument we have for making our government honest and transparent, and of holding it accountable. And I expect members of my administration not simply to live up to the letter but also the spirit of this law.²⁸

After the President's remarks, Attorney General Eric Holder issued a Memorandum that broadened the executive branch's FOIA disclosure policy, and he therefore urged heads of executive departments and agencies to make discretionary disclosures of information:

[A]n agency should not withhold information simply because it may do so legally. I strongly encourage agencies to make discretionary disclosures of information. An agency should not withhold records merely because it can demonstrate, as a technical matter, that the records fall within the scope of a FOIA exemption.²⁹

²⁷ Memorandum from President Barack Obama for the Heads of Exec. Dep'ts and Agencies, *Freedom of Information Act* (Jan. 21, 2009) available at <http://www.whitehouse.gov/the-press-office/freedom-information-act>.

²⁸ President Barack Obama, *Remarks by the President in Welcoming Senior Staff and Cabinet Secretaries to the White House* (Jan. 21, 2009) available at <http://oversight.house.gov/hearing/foia-in-the-21st-century-using-technology-to-improve-transparency-in-government/>.

²⁹ Memorandum from Attorney Gen. Eric Holder for Heads of Exec. Dep'ts and Agencies, *The Freedom of Information Act (FOIA)* (Mar. 19, 2009), available at <http://www.justice.gov/ag/foia-memo-march2009.pdf>.

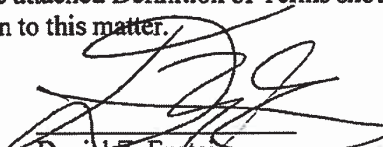
Mr. David C. Shonka
May 3, 2013
Page 9

If it is your position that any portion of the requested information is exempt from disclosure, Cause of Action requests that you provide a detailed justification, specifically identifying the reasons why a particular exemption is relevant and correlating those claims with the particular part of a withheld document to which they apply.

In the event that some portions of the requested information are properly exempt from disclosure, please redact such portions and produce all remaining reasonable segregable non-exempt portions of the requested record.³⁰ If you contend that information contains non-exempt segments, but those non-exempt segments are so dispersed throughout as to make segregation impossible, please state what portion of the document is non-exempt and how the material is dispersed through the document. If a request is denied in full, please outline that it is not possible to segregate portions of the record for release.

In an effort to facilitate record production within the statutory limit, Cause of Action prefers to accept information and/or documents in electronic format (*e.g.*, e-mail, pdf). When necessary, Cause of Action will accept the "rolling production" of information and/or documents, but requests that you provide prompt notification of any intent to produce information on a rolling basis.

If you do not understand this request or any portion thereof, or if you feel you require clarification of this request or any portion thereof, please contact me (Daniel.Epstein@causeofaction.org) immediately at (202) 499-4232. Please note that, for the purposes of responding to this request, the attached Definition of Terms should be interpreted consistently. Thank you for your attention to this matter.



Daniel Z. Epstein
EXECUTIVE DIRECTOR

Encl. Responding to Document Requests, Definitions

³⁰ See 5 U.S.C. § 552(b).

Responding to Document Requests

1. In complying with this request, you should produce all responsive documents that are in your possession, custody or control, whether held by you or your past or present agents, employees and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to Cause of Action.
2. In the event that any entity, organization or individual denoted in this request has been or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. Cause of Action's preference is to receive documents in electronic form (i.e., CD, memory stick or thumb drive) in lieu of paper productions.
4. When you produce documents, you should identify the specific document request or portion thereof in Cause of Action's request to which the documents respond.
5. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
6. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with Cause of Action staff to determine the appropriate format in which to produce the information.
7. If compliance with the request cannot be made in full, compliance shall be made to the extent possible and shall include an explanation of why full compliance is not possible.
8. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
9. If any document responsive to this request was, but no longer is, in your possession, custody or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody or control.
10. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is

otherwise apparent from the context of the request, you should produce all documents which would be responsive as if the date or other descriptive detail were correct.

11. The time period covered by this request is included in the attached request. To the extent a time period is not specified, produce relevant documents from January 3, 2008 to the present.
12. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
13. All documents shall be Bates-stamped sequentially and produced sequentially.

Definitions

1. The term "document" means any written, recorded or graphic matter of any nature whatsoever regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmation, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks and recordings) and other written, printed, typed or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email, regular mail, telexes, releases or otherwise.
3. The terms "and" and "or" shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might

otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

4. The terms "person" or "persons" mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities and all subsidiaries, affiliates, divisions, departments, branches or other units thereof.
5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.