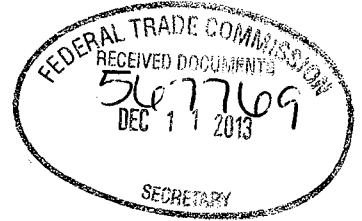


ORIGINAL



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

\_\_\_\_\_  
In the Matter of )  
 )  
LabMD, Inc., )  
a corporation. )  
\_\_\_\_\_ )

DOCKET NO. 9357

PUBLIC

**THIRD-PARTY FORENSIC STRATEGY SERVICES, LLC MOTION FOR  
PROTECTIVE ORDER REGARDING COMPLAINT COUNSEL'S SUBPOENA AD  
TESTIFICANDUM & SUBPOENA DUCES TECUM**

Pursuant to Commission Rule 3.31, 16 C.F.R. § 3.31, Commission Rule 3.31A(e), 16 C.F.R. § 3.31A(e), and Commission Rule 3.34(c), 16 C.F.R. § 3.34(c), Third-Party Forensic Strategy Services, LLC ("LLC"), by and through counsel, hereby moves the Administrative Law Judge ("ALJ") to enter a protective order quashing Complaint Counsel's subpoena *ad testificandum* and subpoena *duces tecum* served upon him.

**INTRODUCTION**

Forensic's employee, Scott Moulton ("Moulton"), serves as LabMD's consultant with regard to the instant litigation, and the litigation it previously initiated, but which has now concluded, against Tiversa Holding Corporation ("Tiversa"). Complaint Counsel's subpoenas for testimony and documents served upon Forensic are in contravention of the terms of the Engagement Letter between Forensic and LabMD, and thus these subpoenas should be quashed. Moreover, Forensic incorporates by reference the arguments made by Respondent LabMD in its recent Motion to Quash and Motion for Protective Order as further reason that the subpoenas served upon it should be quashed.

## FACTS

- A. LabMD retained Forensic as a consultant in anticipation of two separate pieces of litigation: (1) the instant action, and (2) *LabMD v. Tiversa*.

Forensic employs Moulton as a computer forensic specialist. See <http://www.forensicstrategy.com/index.htm>. On July 20, 2011, Respondent LabMD retained Moulton, by way of Forensic, as a consultant in anticipation of two separate pieces of litigation. (Forensic Engagement Letter “Engagement Letter”, attached hereto as Exh. A). The first piece of litigation is the instant one, *i.e. In the matter of LabMD, Inc.*, hereinafter referred to as the “FTC Litigation.” The FTC Litigation includes the FTC’s initial investigation of LabMD which began as early as January 19, 2010. The second piece of litigation is the suit LabMD filed against Tiversa and others, styled *LabMD v. Tiversa et al.*, No. 2011-CV-207137, hereinafter referred to as the “Tiversa Litigation.” Both cases center around P2P technology, and Forensic was alerted by LabMD that Moulton’s analysis would be critical for LabMD to support its claims against Tiversa and to defend itself against the FTC. (Affidavit of Scott Moulton, dated Dec. 11, 2013, attached hereto as Exh. B).

Specifically, Forensic was engaged to “examine equipment, computers, tapes, hard drives, etc. provided [by LabMD and to report its] findings . . .” (Exh. A at 1). The Engagement Letter makes clear that “[a]ny and all work products which [Moulton] produces” in connection therewith is LabMD’s “property...and shall not be expressed in any form to any other party without the express written consent of” LabMD. *Id.* Forensic further obligates itself to “take all reasonable and necessary steps” to prevent disclosure or use of any “Confidential Information” acquired from LabMD, including but not limited to “all information (whether or not reduced to

writing) received or acquired by...incidental to the property, business, undertakings, or affairs of' LabMD. *Id.* LabMD has not waived the protections of the Engagement Letter.

**B. LabMD sued Tiversa, and utilized Forensic's Affidavit to oppose Tiversa's Motion to Dismiss.**

LabMD initiated the Tiversa Litigation against Tiversa in Georgia state court on October 19, 2011. (Complaint attached hereto as Exh. C). This suit was removed to the Northern District of Georgia on January 12, 2012 and Tiversa moved to dismiss. Forensic, and more specifically Moulton, was asked by LabMD to execute an affidavit in support of LabMD's opposition to Tiversa's Motion to Dismiss. (Affidavit of Scott Moulton in Tiversa Litigation, dated Jan. 12, 2012, attached hereto as Exh. D). Specifically, the affidavit was utilized to support LabMD's proposition that the Defendants' actions constituted tortious acts within the state of Georgia, and that its Complaint should not be dismissed on jurisdictional grounds. (LabMD Response to Motion to Dismiss, at 6-7, attached hereto as Exh. E).

The U.S. District Court for the Northern District of Georgia subsequently granted Tiversa's motion to dismiss and LabMD appealed. The Eleventh Circuit affirmed the district court's dismissal. As LabMD did not file a cert petition, the Tiversa Litigation is now terminated. Notably, neither Moulton nor any other Forensic employee was ever designated as an expert witness in this case; rather, Moulton was utilized only as a consultant.

**C. While LabMD has consulted with Forensic regarding the instant litigation, Forensic's employee, Moulton, has not been designated an expert in the instant FTC Litigation.**

The FTC began investigating LabMD as early as January 19, 2010, and initiated its Complaint against LabMD on August 25, 2013. As described *supra*, a primary reason that LabMD retained Forensic, and more specifically Moulton, as a consultant was to provide information necessary to LabMD and its counsel to formulate its defense against the FTC. In the

instant FTC Litigation, Forensic has been made aware that LabMD will not designate Moulton as an expert witness. Furthermore, LabMD will not seek to elicit testimony from Moulton at trial or via deposition, and will not seek to introduce the affidavit he executed in the Tiversa Litigation into evidence. (See Exh. B).

**D. The FTC inappropriately subpoenaed Forensic.**

On October 24, 2013, the FTC subpoenaed Forensic to provide testimony and produce documents in the instant litigation. (See Forensic Subpoena packet, dated Oct. 24, 2013, attached hereto as Exh. F).

The subpoenas *duces tecum* served on Forensic requests:

1. All communications between Forensic and LabMD.
2. All documents considered to prepare the affidavit Forensic executed on January 12, 2012, in the matter captioned LabMD, Inc. v. Tiversa, Inc., Docket no. 11-cv-04044 (N.D. Ga.).
3. All contracts between Forensic and LabMD.
4. All documents related to work Forensic performed for LabMD.
5. All documents related to compensation received by Forensic for services you provided to LabMD.

*Id.* The documents and testimony Complaint Counsel seeks from Forensic are in contravention of the terms of the Engagement Letter and compliance with the subpoenas would violate LabMD's work-product privilege. Furthermore, as discussed in LabMD's Motion to Quash and Motion for Protective Order, the documents and testimony Complaint Counsel seeks from Forensic is sought in contravention of Commission Rule 3.31A(e).

**ARGUMENT**

Third-Party Forensic's motion for protective order against Complaint Counsel is based on the following arguments: (1) The documents and testimony that the FTC seeks from Forensic are in contravention of the terms of the Engagement Letter between Forensic and LabMD; and (2) As previously outlined in LabMD's motion, the documents and testimony that the FTC seeks

from Forensic are sought in contravention of Commission Rule 3.31(e), which states that “a party may not discover facts known or opinions held by an expert who has been retained or specifically employed by another party in anticipation of litigation or preparation for a hearing and who is not listed as a witness for the evidentiary hearing.”

**A. The ALJ should not force Forensic to breach its contract with LabMD, and thereby violate LabMD’s work-product privilege.**

As mentioned above, Forensic entered into an agreement with LabMD regarding the retention of its services. Specifically, Forensic agreed that “[a]ny and all work products which [Moulton] produces” in connection therewith is LabMD’s “property...and shall not be expressed in any form to any other party without the express written consent of” LabMD. (Exh.A). Forensic is further obligated to “take all reasonable and necessary steps” to prevent disclosure or use of any “Confidential Information” acquired from LabMD, including but not limited to “all information (whether or not reduced to writing) received or acquired by...incidental to the property, business, undertakings, or affairs of” LabMD. LabMD has not waived any of its protections under its contract with Forensic, and has no intention of doing so. If Forensic is forced to comply with subpoenas served upon it by the FTC, it will be in breach of its contract with LabMD.

Moreover, if Forensic is forced to comply with the subpoenas, it will produce documents that are in violation of LabMD’s work product privilege. Forensic was retained by LabMD to help develop litigation strategies in support of the Tiversa Litigation, and in defense of the FTC Litigation. (Exh. B and D). Thus, Forensic was retained in anticipation of litigation, and its consultation with LabMD is protected by the work product doctrine. *In re Lab. Corp. of Am.*, 2011 FTC LEXIS 30, \*9-10 (F.T.C. Feb. 24, 2011)(citations omitted)(emphasis added). If Forensic complies with the subpoenas, it will not only be subjected to liability to LabMD for

breach of contract, but also for violating LabMD's work product privilege. Courts have held that a subpoena must be quashed by the issuing court if compliance would subject the responding party "to liability to another person for violating a privilege." *Hackmann v. Auto Owners Ins. Co.*, 2009 U.S. Dist. LEXIS 15128, at \*2 (S.D. Ohio Feb. 6, 2009). Likewise, the subpoenas served upon Forensic should be quashed because compliance would subject it to liability to LabMD for violating its work product privilege.

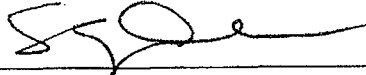
**B. Documents and testimony that the FTC seeks from Forensic are sought in contravention of Commission Rule 3.31A(e), and should be protected from production.**

Commission Rule 3.31A(e), 16 C.F.R. § 3.31A(e) mandates that "a party may not discover facts or opinions held by an expert who has been retained or specifically employed by another party in anticipation of litigation or preparation of hearing and who is not listed as a witness for the evidentiary hearing." To the extent that Forensic's employee, Moulton, is considered an expert in the instant litigation, he is an expert consultant. He is not an expert witness, and LabMD will not seek to elicit testimony from Moulton at trial or via deposition. Furthermore, LabMD will not seek to introduce the affidavit he executed in the Tiversa Litigation into evidence. (Exh.B). Thus, the FTC is prohibited by the Commission rules from subpoenaing information from Moulton or Forensic regarding facts known or opinions held about the FTC Litigation.

**CONCLUSION**

For the foregoing reasons, Forensic respectfully requests that a protective order is entered quashing the subpoena *ad testificandum* and subpoena *duces tecum* served upon it.

Respectfully submitted,



---

Elizabeth G. Howard  
Georgia Bar No. 100118  
Barrickman, Allred & Young, LLC  
5775 Glenridge Drive, NE, Suite E-100  
Atlanta, GA 30328  
Telephone: (404) 252-2230  
Fax: (404) 252-3376  
[egh@bayatl.com](mailto:egh@bayatl.com)

Dated: 12/11/13

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

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

**PROPOSED ORDER GRANTING THIRD-PARTY FORENSIC STRATEGY SERVICES, LLC MOTION FOR PROTECTIVE ORDER REGARDING COMPLAINT COUNSEL'S SUBPOENAS SERVED UPON IT**

This matter came before the Administrative Law Judge on December 11, 2013, upon a Motion for Protective Order regarding Complaint Counsel's subpoenas served upon Forensic Strategy Services, LLC ("Forensic"). Having considered Forensic's Motions and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that Forensic's Motion is GRANTED and that the subpoena *testificandum* and subpoena *duces tecum* served upon it are quashed.

ORDERED:

\_\_\_\_\_  
D. Michael Chappell  
Chief Administrative Law Judge

Date:



Forensic Strategy Services, LLC.  
601-B Industrial Court Woodstock,  
Georgia 30189

Phone 770-926-5588  
Fax 770-926-7089  
Web [forensicstrategy.com](http://forensicstrategy.com)

## Engagement Letter

DATE: July 20, 2011

This letter is to set forth the terms and objectives of our proposed engagement and the nature and limitations of the services we will provide to your company until mutually changed.

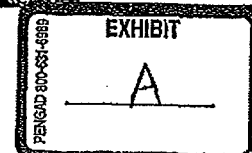
### SCOPE OF WORK

**A. Scope Limitations.** We will examine equipment, computers, tapes, hard drives, etc. provided and reports our findings based on any requests. We will create an unmodified clone of any hard drives we receive if necessary for examination.

**B. Agreed Upon Services.** We will work for your firm as a consulting specialist and a part of your research staff. All material is confidential between Forensic Strategy and your Company. We hope to better meet your expectations of service by having you clearly identify what items specifically you wish reviewed. There is no guarantee that what you are asking for actually exists; We will only report on what actually exists.

### Confidentiality Clause:

- a. The Client wishes to engage the Consultant to provide grant consulting services according to this engagement letter;
- b. The Client wishes to identify its specific responsibilities and to provide for confidentiality of any information relating to this agreement; and
- c. The Consultant represents that they are duly licensed as a LLC and valid under the State of Georgia;
- d. Any and all work products which the Consultant produces to fulfill the terms of the Statement of Work shall be the property of the Client and shall not be expressed in any form to any other party without the express written consent of the Client.
- e. The Consultant and its designate, shall at all times, both during and after the term of this Agreement, take all reasonable and necessary steps to ensure that both the Consultant, and any of their agents, employees, independent Consultants, or other representatives maintain in confidence and do not disclose or permit disclosure (via any action or inaction) of any Confidential Information to any entity or utilize any Confidential Information, except as may be required to perform the services under this Agreement.
- f. For the purposes of this Agreement "Confidential Information" shall include all information (whether or not reduced to writing), received or acquired by the Consultant or any of their agents, employees, independent Consultants, or other representatives during the term of this Agreement, or incidental to the property, business, undertakings, or affairs of:
  - a. the Client; and
  - b. the Client's proprietary knowledge with the exception only of information which is public or becomes public information through no action of the Consultant and information which is received from another entity lawfully in possession of the information and under no obligation to keep the information confidential.
- g. Immediately upon completion of the services provided for hereunder, the Consultant shall download from its computers and store in a safe location all originals and copies of any documentation relating to said Services and any other Confidential Information in its possession or control.



Forensic Strategy Services, LLC.  
601-B Industrial Court  
Woodstock, Georgia 30189

Phone 770-926-5588  
Fax 770-926-7089  
Web [forensicstrategy.com](http://forensicstrategy.com)

- h. This Agreement shall constitute the sole contract between the Consultant and the Client and shall commence on the date of signing (below). In the event of renewal, the provisions of this agreement shall govern unless otherwise amended in writing, signed by both parties.

#### FEE SCHEDULE

This letter is to set forth the terms and objectives of our proposed engagement and the nature and limitations of the services we will provide to your company until mutually changed.

- A. **Professional Fees.** The engagement fee for these services will be \$3000. This engagement will reserve 10 hours of my time and is non-refundable and all items will be billed against this including drive time, review time, examining evidence, etc. Following the 10 hours all time will be billed at the professional fee of \$300 an hour plus expenses.
- B. If there are any additional material needed, such as hard drives, photos, etc there will be an additional charge for those items and you will be billed for them.
- C. If there is a need for data to be stored; there will be a charge for each hard drive necessary. Any additional research needed after initial assessment will also be billed at the hourly rate provided Forensic Strategy Services LLC ("Forensic") has exceeded the ten (10) hours of work outlined in Section A above. In the event Forensic has not exceeded the ten (10) hours of work outlined in Section A above, Forensic will apply any research needed after the initial assessment to the ten (10) hours of time provided for in Section A above and then bill client at the applicable hourly rate. Any additional time to be billed to client in excess of the ten (10) hours of time provided for in Section A above must be first approved by Client.
- D. Any additional items needed after the initial image, and index and basic review and phone call reporting the findings will be charged at \$300 per hour and the client will be informed at what point that begins. Any additional time to be billed to client in excess of the ten (10) hours of time provided for in Section A above must be first approved by Client.
- E. If Scott Moulton or anyone from Forensic Strategy Services or representative of the company in any way is called by any party in response to this agreement for any reason, or subpoena for any reason due to this engagement, you as the party are responsible for all time and expenses. These items will be billed to you at \$300 an hour and to be prepaid in advance of testimony at a cost of reserving each day at \$2000 per a day to alleviate any time including waiting, or preparation, or testimony on the stand.

**B. Factors Affecting Your Professional Fee.** Professional fees will be based upon several factors; the most important of which includes time and labor involved, skill requisite to perform the professional services properly, and any special circumstances imposed.

There are additional costs for storage of data and equipment. This is dependant on the amount of data and number of systems needing to be stored and maintained. These prices will vary in accordance with the items and will be discussed as needed.

**C. Direct Expenses.** Additional charges for computer services, fax transmissions, report production, and out of pocket costs, including travel costs, will be added to our professional fees. There are additional charges for color documents and color copies. Such charges are in addition to any estimated fees given and will be due and payable upon presentation as billed.

#### TERMINATION

**Right to Terminate.** Either party may terminate this relationship at any time by any form of written notification including email with confirmation by both parties.

#### LIMIT OF LIABILITY

Both parties agree that liability hereunder for damages, regardless of the form of action, shall not exceed the total amount paid for the services described herein. This shall be either party's exclusive remedy.

Both parties further agree that neither party shall be liable for any lost profits, or for any claim or demand against it by any other party. In no event will either party be liable for incidental or consequential damages even if it has been advised of the possibility of such damages.

No action, regardless of form, arising out of the services under this agreement, may be brought

Forensic Strategy Services, LLC.  
601-B Industrial Court  
Woodstock, Georgia 30189

Phone 770-926-5588  
Fax 770-926-7089  
Web [forensicstrategy.com](http://forensicstrategy.com)

by either party more than one year after the date of the last services provided under this agreement.


**APPLICABLE LAW**


This engagement letter shall be governed as to validity, interpretation, construction, effect and in all other respects by the laws and decisions of the state of Georgia. In the event of commencement of any legal action regarding any term or condition of this engagement such action by agreement is to be subject to the jurisdiction of the courts of Georgia.

**COMPLETE AGREEMENT**

This letter comprises the complete and exclusive statement of the agreement between the parties, superseding all proposals oral or written and all other communications between the parties. If any provision of this letter is determined to be unenforceable, all other provisions shall remain in force. If you have any questions or concerns regarding this engagement letter or desired services, Please contact us at the above address.

Agreed on behalf of Client:

Signature:   
Date: July 20, 2011  
Print Name: Michael J. Daugherty  
Title: President LabMD, Inc. *General Counsel*

Accepted for Forensic Strategy Services, LLC  
Company Officer Signature:   
Date: \_\_\_\_\_  
Print Name: \_\_\_\_\_  
Title: \_\_\_\_\_

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

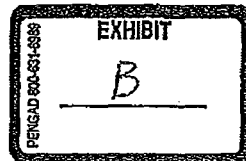
In the Matter of	)	
	)	
LabMD, Inc.	)	Docket No. 9357
	)	
	)	

AFFIDAVIT OF SCOTT MOULTON

\*\*\*\*\*

The Affiant, Scott Moulton, having been duly sworn, hereby states and alleges as follows:

1. My name is Scott Moulton, and I am a computer forensic specialist and the CEO of Forensic Strategy Services, LLC ("Forensic"). I have personal knowledge of the matters discussed and alleged herein.
2. On July 20, 2011, LabMD, Inc. ("LabMD") retained me as a consultant in anticipation of litigation to aid it and its attorneys in responding to an investigation initiated by the FTC, as well as any potential litigation that could result against LabMD by the FTC.
3. I was also hired to provide analysis and information necessary to LabMD and its counsel to formulate litigation strategies in support of its claims against Tiversa Holding Corporation ("Tiversa").
4. LabMD sued Tiversa in Georgia state court on October 19, 2011 in the case styled *LabMD v. Tiversa, et.al*, No. 2011-cv-207137, hereafter referred to as the "Tiversa Litigation."
5. The FTC initiated the instant litigation against LabMD on August 25, 2013.
6. I executed an affidavit in the Tiversa Litigation to support LabMD's proposition that Tiversa and the other defendants committed tortious acts in the state of Georgia, and thus the case should not be dismissed on jurisdictional grounds.




7. I have been made aware that LabMD will not designate me or Forensic as an expert witness in the instant litigation. Moreover, LabMD will not seek to elicit testimony from me or Forensic at trial or via deposition, and will not seek to introduce the affidavit that I executed in the Tiversa Litigation into evidence.

FURTHER AFFIANT SAYETH NAUGHT.

  
SCOTT MOULTON

County of Cherokee )  
Georgia ) :ss

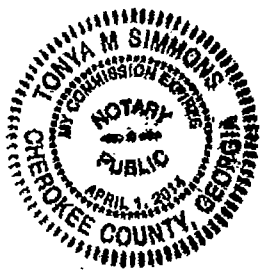
The foregoing instrument was acknowledged before me this 11th day of December, 2013, by SCOTT MOULTON, of Forensic Strategy Services, Inc.

  
Tonya M Simmons

Notary Public

My Commission expires: April 1, 2014

545700v1

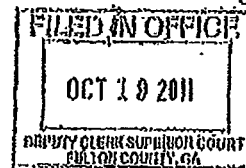




IN THE SUPERIOR COURT OF FULTON COUNTY  
STATE OF GEORGIA

LABMD, INC., a Georgia Corporation, )  
 Plaintiff, )  
 v. )  
 TIVERSA, INC., a Pennsylvania Corporation, )  
 TRUSTEES OF DARTMOUTH COLLEGE, and )  
 M. ERIC JOHNSON, )  
 Defendants. )

CIVIL ACTION  
FILE NO:  
2011CV207137



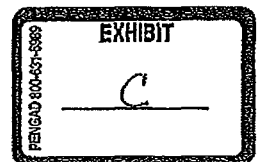
COMPLAINT

Plaintiff LabMD, Inc. ("Plaintiff" or "LabMD") hereby files this Complaint against Tiversa, Inc., a Pennsylvania Corporation ("Tiversa"), Trustees of Dartmouth College ("Dartmouth") and M. Eric Johnson ("Johnson") (Tiversa, Dartmouth and Johnson collectively referred to herein as "Defendants") to show this Honorable Court the following:

PARTIES, VENUE, AND JURISDICTION

I.

LabMD, Inc. is a domestic corporation organized under the laws of the State of Georgia with a principal office address of 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339.



2.

Defendant Tiversa, Inc. is a corporation organized under the laws of the State of Pennsylvania. Defendant Tiversa can be served with process through Robert Boback, Tiversa's President, at 144 Emeryville Drive Suite 300, Cranberry Township PA 16066

3.

Defendant M. Eric Johnson is an individual over the age of 18 and can be served with process at Tuck School of Business at Dartmouth College, 100 Tuck Hall, Hanover, New Hampshire 03755.

4.

Defendant Trustees of Dartmouth College are organized according to the laws of the state of New Hampshire and may be served with process at 14 S Main Street 2C, Hanover NH 03755.

5.

Defendants performed certain actions contained herein at 1117 Perimeter Center West, Atlanta, Fulton County, Georgia 30338 ("LabMD Office").

6.

Defendants took deliberate actions at LabMD's office and, as such, created continuing obligations to Georgia residents, including LabMD.

7.

Defendant Tiversa solicited business from LabMD on six separate occasions without any request from LabMD. Solicitation One, Solicitation Two, Solicitation Three,

Solicitation Four, Solicitation Five and Solicitation Six (as defined herein) all occurred at the LabMD Office.

8.

LabMD's causes of action against Defendants arise out of and result from Defendants' actions within Georgia.

9.

Exercising jurisdiction over Defendants is consistent with due process notions of fair play and substantial justice.

10.

Defendants transacted business within the State of Georgia.

11.

Defendants committed tortious acts within the State of Georgia.

12.

Defendants regularly do business in the State of Georgia.

13.

Defendants engage in a persistent course of conduct within the State of Georgia.

14.

Defendants derive substantial revenue from services rendered in the State of Georgia.



15.

Defendants took personal property belonging to LabMD which was in the State of Georgia.

16.

This Court has jurisdiction over the parties and the subject matter of this action.

17.

Venue is proper in this Court.

**DEFENDANTS' PATTERN AND PRACTICES**

18.

Tiversa provides peer-to-peer ("P2P") intelligence services to corporations, government agencies and individuals based on patented technologies that can monitor over 550 million computer users daily.

19.

Requiring no software or hardware, Tiversa can search for, locate, copy, download and determine the source of a person's computer files utilizing its "patented technologies."

20.

Tiversa offers a Corporate Breach Protection product which establishes a long-term, real-time monitoring program that detects and records customer-specific computer searches, data loss exposures, and corporate intellectual property loss on P2P networks twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year.

21.

Tiversa's patented EagleVision X1™ technology globally indexes internet and file-sharing networks in real-time.

22.

According to Tiversa's website, "Tiversa's blend of automated, patented technology and deep expertise... enables [it] to pinpoint the disclosure source involved in the exposure of data."

23.

According to Tiversa's website, as part of a comprehensive breach investigation, Tiversa can conduct an in-depth network scan to determine file proliferation across P2P file sharing networks to identify the location of a person's computer files.

24.

Defendant Johnson is Director of Tuck School of Business' Glassmeyer/McNamee Center for Digital Strategies ("McNamee Center").

25.

The Tuck School of Business is the business school of Dartmouth College.

26.

Defendant Johnson accepted federal funds from the National Institute of Standards and Technology, the United States Department of Justice, the United States Department of Homeland Security, the National Science Foundation and other federal/state/local governments in furtherance of his position as Director of the McNamee Center and those activities described herein.

27.

Defendant Dartmouth accepted federal funds from the National Institute of Standards and Technology, the United States Department of Justice, the United States Department of Homeland Security, the National Science Foundation and other federal/state/local governments in furtherance of Defendant's position as Director of the McNamara Center and those activities described herein.

28.

Defendant Tiversa accepted federal funds from the National Institute of Standards and Technology, the United States Department of Justice, the United States Department of Homeland Security, the National Science Foundation and other federal/state/local governments in furtherance of its activities, including those activities described herein.

29.

In as early as 2007, Defendants worked in concert and intentionally to search the internet and computer networks for computer files containing personally identifiable information.

30.

On July 24, 2007, Defendant Johnson testified before the United States House of Representatives Committee on Oversight and Government Reform ("2007 Committee Hearing"). In his testimony, Defendant Johnson admitted that he, in concert with Defendant Tiversa, intentionally posted the text of an e-mail containing an active Visa debit number and AT&T phone card in a music directory that was shared via

LineWire. Defendants Johnson and Tiversa observed the activity on the file and tracked it across P2P networks.

31.

Defendant Johnson further testified in the 2007 Committee Hearing that he and Tiversa "intentionally searched and downloaded thousands of bank-related documents circulating on the [P2P] networks," including, but not limited to, bank statements and completed loan application forms which "contained enough information to easily commit identity theft or fraud."

32.

Defendant Johnson also testified during the 2007 Committee Hearing that he and Tiversa, in concert, intentionally searched and downloaded "performance evaluations, customer lists, spreadsheets with customer information, and clearly marked confidential bank material."

33.

During the 2007 Committee Hearing, Defendant Tiversa admitted that it "developed technology that would allow it to position itself throughout the various P2P networks" and view all searches and information available on P2P networks. A true and correct copy of the 2007 testimony from Defendant Tiversa is attached hereto as Exhibit A.

34.

During the 2007 Committee Hearing, Defendant Tiversa admitted that its proprietary software allowed it to process 300 million searches per day, over 170 million more searches than Google was processing per day. *See* Exhibit A.

35.

During the 2007 Committee Hearing, Defendant Tiversa admitted that its proprietary technology allows it to not only process all of the search requests over the internet but also to view the information available on the networks, including computer files containing personally identifiable information ("PII") and protected health information ("PHI"). *Id.*

36.

During the 2007 Committee Hearing, Defendant Tiversa admitted that it intentionally searched for and downloaded computer files containing "federal and state identification, including passports, driver's licenses, Social Security cards, dispute letters with banks, credit card companies, insurance companies, copies of credit reports--Experian, TransUnion, Equifax, individual bank card statements and credit card statements, signed copies of health insurance cards, full copies of tax returns, active user names and passwords for online banking and brokerage accounts and confidential medical histories and records." *Id.*

37.

In April, 2009, Defendant Johnson, in concert with Defendants Tiversa and Dartmouth, published an article entitled *Data Hemorrhages in the Health-Care Sector* ("Johnson Paper"). A true and correct copy of the Johnson paper is attached hereto as Exhibit B.

38.

The Johnson Paper was based upon activities "conducted in collaboration with Tiversa who has developed a patent-pending technology that, in real-time, monitors global P2P sharing networks." See Exhibit B.

39.

The Johnson Paper was partially supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001 under the auspices of the Institute for Information Infrastructure Protection (I3P). *Id.*

40.

According to the Johnson Paper, Defendants Johnson and Tiversa initially searched P2P networks "looking for files from top ten publically traded health-care firms" and "randomly gathered a sample of shared files related to health care and those institutions" (the "Initial Search"). *Id.*

41.

Defendant "Tiversa's servers and software allowed [Johnson and Tiversa] to sample in the four most popular networks (each of which supports the most popular clients) including Gnutella (e.g. Limewire, BearShare), FastTrack (e.g., KaZaA,

Grokster), Aries (Aries Galaxy), and e-donkey (e.g. eMule, EDonkey2K)" according to the Johnson Paper. *Id.*

42.

Defendants Johnson and Tiversa "captured" files containing PHI or PII during the Initial Search. *Id.*

43.

Defendants Johnson and Tiversa admitted to intentionally searching for, downloading and "manually" analyzing 3,328 computer files belonging to publically traded health care firms as part of the Initial Search. *Id.*

44.

Defendants Johnson and Tiversa intentionally searched for, downloaded and opened patient-generated spreadsheets containing details of medical treatments and costs, government applications for employment containing detailed background information, social security numbers, dates of birth, places of birth, mother's maiden name, history of residences and acquaintances, schooling history, employment history and other data which, according to Defendant Johnson, "could be used to commit medical or financial identity theft" as part of the Initial Search. *Id.*

45.

Defendants Johnson and Tiversa used the data downloaded during the Initial Search to intentionally search for computer files on computer hosts that Defendants "had found other dangerous data" previously (the "Second Search"). *Id.*

46.

During the Second Search, Defendants Johnson and Tiversa "found a 1,718-page document containing patient Social Security numbers, insurance information, and treatment codes" ("1,718 File"). *Id.*

47.

The Johnson Paper included a "redacted excerpt" of the 1,718 File. *Id.*

48.

The 1,718 File was created on a LabMD computer.

49.

The 1,718 File was stored on a LabMD computer.

50.

The 1,718 File was the personal property of LabMD, Inc.

51.

Numerous other computer files containing PHI and PII were intentionally searched for, downloaded and opened by Defendants Tiversa and Johnson as part of the Johnson Paper. *Id.*

52.

During an interview following the publication of the Johnson Paper, Defendant Johnson publically admitted to intentionally searching major computer networks to locate computer files containing PHI belonging to certain top ten publicly traded healthcare firms across the United States.



53.

During an interview following the publication of the Johnson Paper, Defendant Johnson publically admitted to "looking for" computer files containing PHI and PII.

54.

During an interview following the publication of the Johnson Paper, Defendant Johnson publically admitted to intentionally searching major computer networks in "a rather casual way," over a six month period to locate "promising areas," "places" or search terms which would lead to the download of computer files containing personal health information.

55.

During an interview following the publication of the Johnson Paper, Defendant Johnson publically admitted to intentionally downloading and opening computer files containing over 20,000 medical patient records, "and for those patients, 82 fields of information, not just name, date, social security numbers...but a much more detailed set of information, including their employer, their insurance carrier, the doctor that was treating them, [and] the diagnostic codes that were used."

56.

On May 4, 2009, Defendant Tiversa testified before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection ("2009 CTC Hearing"). A true and correct copy of the 2009 CTC Hearing testimony is attached hereto as Exhibit C.

57.

During the 2009 CTC Hearing, Tiversa testified that, through the use of its proprietary software, it "can see and detect all previously undetected activity" and "where an individual user can only see a very small portion of a P2P file sharing network, [it] can see the P2P network in its entirety in real time. [It] has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (*Information Week*) to refer to Tiversa as the "Google of P2P." See Exhibit C (emphasis added).

58.

During the 2009 CTC Hearing, Tiversa did a "live demonstration" utilizing its proprietary technology whereby it intentionally searched for and downloaded over 276,000 tax returns. *Id.*

59.

During the 2009 CTC Hearing, Tiversa testified that between February 25, 2009 and April 26, 2009, it had "downloaded 3,908,060 files" from P2P networks, some of which contained PHI and PII. *Id.*

60.

During the 2009 CTC Hearing, Tiversa produced redacted copies of computer files it downloaded from P2P networks containing PHI and PII. *Id.*

61.

During the 2009 CTC Hearing, Tiversa produced the 1,718 File and testified about the 1,718 File. *Id.*

62.

Tiversa did not redact the first name, date of birth or group insurance number when it produced the LabMD File at the 2009 CTC Hearing.

63.

Between July 13-27, 2009, Defendants Tiversa and Johnson intentionally searched for and downloaded approximately 7,911 computer files containing PII and/or PHI from twenty-five (25) top medical research institutions. *Id.*

64.

Between July 13-27, 2009, Defendants Tiversa and Johnson intentionally opened approximately 2,966 computer files from twenty-five (25) top medical research institutions, some of which contained PII and/or PHI, including nursing notes, medical histories, patient diagnoses, psychiatric evaluations, letters to patients and spreadsheets with patient data. *Id.*

65.

On July 29, 2009, Tiversa appeared before the United States House of Representatives Committee on Oversight and Government Reform ("2009 COG Hearing") and testified that it had the technology to search and download files from P2P networks even where a company has "the most robust security measures," including "firewalls, anti-virus [sic], intrusion detection, intrusion prevention, and

encryption." A true and correct copy of the 2009 COG Hearing testimony is attached hereto as Exhibit D.

66.

During the 2009 COG Hearing, Tiversa intentionally searched for and downloaded tax returns containing PII in "live time." See Exhibit D.

67.

During the 2009 COG Hearing, a hearing open to the general public, Tiversa revealed the social security numbers from tax returns based upon its "live time" demonstration. *Id.*

68.

During the 2009 COG Hearing, Tiversa testified that "beginning in 2003, [it] developed systems that monitor and interact with and within P2P networks to search for sensitive information. . ." *Id.*

69.

During the 2009 COG Hearing, Tiversa testified that it searched for and downloaded files containing PII and PHI as part of a research project. *Id.*

70.

Between September 23-October 7, 2009, Defendants Tiversa and Johnson intentionally searched for and downloaded computer files containing PII and/or PHI from medical research institutions.

71.

Between September 23-October 7, 2009, Defendants Tiversa and Johnson intentionally opened computer files from medical research institutions, some of which contained PHI and/or PII, including files with social security numbers, dates of birth and diagnoses codes.

DEFENDANT TIVERSA'S SOLICITATIONS AND ACTIONS

72.

On May 13, 2008, Robert Boback, CEO of Defendant Tiversa, called LabMD (the "Tiversa Call").

73.

During the Tiversa Call, Mr. Boback informed LabMD that he was calling because he was in possession of a computer file containing patient social security numbers and the computer file belonged to LabMD.

74.

During the Tiversa Call, Mr. Boback told LabMD that the computer file in his possession was the type of file individuals were searching for on P2P networks.

75.

During the Tiversa Call, Mr. Boback told LabMD that large financial institutions and medical insurance companies were being targeted by individuals searching for and downloading computer files containing PHI and PII.

76.

During the Tiversa Call, Mr. Boback agreed to provide a copy of the computer file in its possession to LabMD.

77.

On May 13, 2008 at approximately 11:25 AM EST, Defendant Tiversa emailed a copy of the file in its possession to LabMD (the "11:25 Email"). A true and correct copy of the 11:25 Email is attached hereto as Exhibit E.

78.

The file produced in the 11:25 Email was the LabMD File.

79.

In the 11:25 email, Defendant Tiversa agreed to have an engineer review the computer file in its possession to "see when [its] systems first detected/downloaded the file from P2P network." See Exhibit E (emphasis added).

80.

On May 13, 2008, at approximately 1:22 PM EST, Mr. Boback again emailed LabMD (the "1:22 Email"). A true and correct copy of the 1:22 Email is attached hereto as Exhibit F.

81.

In the 1:22 Email, Defendant Tiversa informed LabMD that "it checked back against the timeline to see the date that [it] originally acquired the file pertaining to LabMD" and "it appears" that Defendant Tiversa "first downloaded the file on 02/05/08 at 3:49PM." See Exhibit F (emphasis added).

82.

In the 1:22 Email, Defendant Tiversa informed LabMD that its "systems show a record of continued availability for sporadic periods over the past month" but that it had not attempted to download the 1,718 File again. *Id.*

83.

In the 1:22 Email, Defendant Tiversa informed LabMD that Tiversa's "system did not auto-record the IP...most likely due to the limited amount of criteria indexed against the DSP." According to Defendant Tiversa, it may "have the actual source IP address in the data store logs but it was not readily available at this point" and it "should be able to get it but it would take some time." *Id.*

84.

On May 13, 2008 at approximately 2:13 PM EST, Defendant Tiversa solicited business from LabMD (the "Solicitation of Services"). A true and correct copy of the Solicitation of Services is attached hereto as Exhibit G.

85.

In the Solicitation of Services, Defendant Tiversa offered to "provide investigative and remediation services through [its] Incident Response Team" if LabMD was in need of Defendant Tiversa's "professional assistance." See Exhibit G.

86.

In the Solicitation of Services, Defendant Tiversa offered to "locate and identify the precise source where it downloaded the 1,718 File and could "identify additional disclosed files from that source (of which there are most likely additional files since

most individuals are sharing an average of over 100 files per PC)." Additionally, Defendant Tiversa offered to "perform a Global Spread Analysis." Finally, and according to Defendant Tiversa, "most importantly, [it could] work to recover and cleanse the sensitive documents from the P2P." *Id.* In closing, Defendant Tiversa offered to put LabMD "in touch with [Tiversa's] Operations team" if any of Tiversa's "services [were] of interest" to LabMD. *Id.*

87.

On May 15, 2008 at approximately 4:34 AM EST, LabMD asked Defendant Tiversa for specific information regarding the means it searched for and downloaded the 1,718 File. Defendant Tiversa informed LabMD that any information regarding the means by which it acquired LabMD's file "would require a professional services agreement" and that there were "many more necessary benefits to a proper investigation" by Defendant Tiversa (the Second Solicitation"). A true and correct copy of the Second Solicitation is attached hereto as Exhibit H.

88.

On May 22, 2008, without prompting or contact from LabMD, Defendant Tiversa sent an email to LabMD indicating that "it continued to see people searching for the file in question on the P2P network" and that Defendant Tiversa's system "recorded that the file still exists on the network. . . although [it] had not attempted to download another copy." Defendant Tiversa again solicited business from LabMD and asked LabMD if it needed "some assistance" and again offered Tiversa's "Incidence Response



Services" (the Third Solicitation"). A true and correct copy of the Third Solicitation is attached hereto as Exhibit I.<sup>1</sup>

89.

In the Third Solicitation, Defendant Tiversa outlined the costs, turn around time and potential outcome that LabMD could expect if it engaged the services of Defendant Tiversa. *Id.*

90.

On May 23, 2008 at approximately 10:08 AM EST, Defendant Tiversa transmitted a services agreement and confidentiality agreement to LabMD. *Id.* A true and correct copy of the Services Agreement and Confidentiality Agreement are attached hereto as Exhibit J.

91.

On May 30, 2008, Defendant Tiversa solicited the business of LabMD for a fourth time and informed LabMD that if the terms of the Services Agreement and Confidentiality Agreement were acceptable to LabMD, Defendant "Tiversa should get started right away due to the sensitivity of the file" that was in its possession and further informed LabMD that the "title of the file [in its possession] had 'insurance aging' in it, which is being highly sought after" (the "Fourth Solicitation"). A true and correct copy of the Fourth Solicitation is attached hereto as Exhibit K.

<sup>1</sup> A series of email exchanges are contained in Exhibit I for the Court's convenience. The first email LabMD received from Defendant Tiversa, dated May 22, 2008 at 3:22 PM EST is contained on page 3 of 4 of Exhibit I and the email exchange continues in reverse chronological order based upon this first communication.

92.

On June 6, 2008, Defendant Tiversa solicited business from LabMD for a fifth time (the "Fifth Solicitation"). A true and correct copy of the Fifth Solicitation is attached hereto as Exhibit L.

93.

In the Fifth Solicitation, Defendant Tiversa stated the following:

I hope this email finds you doing well. I wanted to follow-up with you as I have not heard anything regarding the disclosure at LabMD. I am not sure if you caught the recent press about Walter Reed Army Medical Center having a disclosure of over 1000 patients SSNs etc. The story of the disclosure has been picked up by over 200 publications. Since then, we have seen the usual increase in search activity on the P2R (presumably media) in attempt [sic] to find this and other information of this type. Given this fact, we should move to remediation very quickly. If you have been able to locate the source of the disclosure internally, that would be helpful. The file, however, will most likely have been already taken by secondary disclosure points which will need to be found and remediated. Please let me know if you need assistance.

See Exhibit L.

94.

On July 15, 2008 at 10:03 AM EST, Defendant Tiversa solicited business from LabMD for a sixth time and stated the following:

I wanted to follow-up with you regarding the breach that we discussed several weeks ago. We have continued to see individuals searching for and downloading copies of the file that was provided. . . it is important to note that LabMD is not the only company that has been affected by this type of breach. This is widespread problem that affects tens of thousands of organizations and millions of individuals. I am not sure if you read the Washington Post, but there was an [sic] front page article last week involving a widely reported file sharing breach of Supreme Court Justice

Stephen Breyer's SSN and personal data. Wagner Resources, the investment firm responsible, took immediate action to solve the problem which resonated with the affected individuals. In fact, many of the individuals whose information was disclosed contacted the owner of the firm to say that HB was the victim of this relatively unknown, although dangerous, security risk.

(the "Seventh Solicitation"). A true and correct copy of the Seventh Solicitation is attached hereto as Exhibit M.

95.

In response to the Sixth Solicitation, LabMD directed Defendant Tiversa to LabMD's attorneys.

96.

On September 30, 2010, LabMD, through the undersigned, demanded return of the 1,718 File from Defendant Tiversa. A true and correct copy of the September 30, 2010, correspondence from LabMD to Defendant Tiversa is attached hereto as Exhibit N.

97.

On September 30, 2010, LabMD, through the undersigned, demanded return of the 1,718 File from Defendant Johnson. A true and correct copy of the September 30, 2010, correspondence from LabMD to Defendant Johnson is attached hereto as Exhibit O.

98.

On September 30, 2010, LabMD, through the undersigned, demanded return of the 1,718 Pile from Defendant Dartmouth. A true and correct copy of the September 30, 2010, correspondence from LabMD to Defendant is attached hereto as Exhibit P.

99.

Defendants Johnson and Dartmouth continue to financially benefit from the searching for, downloading and opening of computer files containing PHI and PII from third parties.

100.

Defendants Johnson and Dartmouth discussed all of the activities referenced herein in a 2011 paper presented at the 44<sup>th</sup> annual Hawaii International Conference on System Sciences entitled *Will HITECH Heal Patient Data Hemorrhages*. A true and correct copy of the Hawaii International Conference paper is attached hereto as Exhibit Q.

101.

Defendants Johnson and Dartmouth discussed the activities referenced herein in an article entitled *Usability Failures and Healthcare Data Hemorrhages* published in the March/April 2011 issue of the IEEE *Security and Privacy* magazine. A true and correct copy of the IEEE article is attached hereto as Exhibit R.

102.

Defendants received federal funding and used federal funding to perform the activities referenced herein.

103.

As of October 13, 2011, a link to the Johnson Paper appears on the Tuck homepage on the world wide web along with links to Johnson's other articles referenced herein. A true and correct copy of a screenshot of Tuck's homepage taken on October 13, 2011, is attached hereto as Exhibit S.

COUNT I: COMPUTER FRAUD AND ABUSE ACT (18 USC § 1030)  
(Defendants Tiversa and Johnson Only)

104.

LabMD realleges the allegations contained in Paragraphs 1-103 as though stated herein verbatim.

105.

LabMD's computers are used in and affect interstate commerce.

106.

Defendant Tiversa intentionally accesses LabMD's computers and networks and downloaded the 1,718 File without authorization.

107.

Defendant Tiversa exceeded any authorizations, if any, it had to access LabMD's computers and networks and downloaded the 1,718 File.

108.

Defendant Johnson intentionally accesses LabMD's computers and networks and downloaded the 1,718 File without authorization.

109.

Defendant Johnson exceeded any authorizations, if any, it had to access LabMD's networks and computers.

110.

Defendant Tiversa transmitted the 1,718 File across state lines in the furtherance of interstate commerce.

111.

Defendant Johnson transmitted the 1,718 File across state lines in the furtherance of interstate commerce.

112.

Defendant Tiversa accessed LabMD's computers and networks with the intent to extort money from LabMD.

113.

Defendant Tiversa impaired the confidentiality of information obtained from LabMD's computers without authorization or by exceeding any authorized access, to the extent any authorization existed.

114.

Defendant Tiversa demanded and/or requested money or other thing of value from LabMD during the First, Second, Third, Fourth, Fifth and Sixth Solicitation.

115.

Tiversa's demands and/or requests for money or other things of value were a direct result of Tiversa's download of the 1,718 File.

116.

Tiversa downloaded the 1,718 File from LabMD's computer in order to facilitate the extortion of money and/or items of value from LabMD.

117.

LabMD suffered and continues to suffer damages as a result of the above actions in an amount to be proven at trial.

**COUNT II: COMPUTER CRIMES (O.C.G.A. 16-9-93)**  
**(Defendants Tiversa and Johnson Only)**

118.

LabMD realleges the allegations contained in Paragraphs 1 through 117 as though stated hererin verbatim.

119.

O.C.G.A. 16-9-93(a) provides that "[a]ny person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession. . . [or] (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

120.

O.C.G.A. 16-9-93(c) provides that "any person who uses a computer or computer network with the intention of examining any employment, medical, salary,

credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy."

121.

O.C.G.A. 16-9-93 (g)(1) provides that "any person whose property or person is injured by reason of a violation of any provision of [O.C.G.A. 16-9-93] may sue therefore and recover for any damages sustained and the costs of suit."

122.

Defendant Tiversa used a computer network to search for, download, open and disseminate the 1,718 File.

123.

Defendant Tiversa knew that the searching for, downloading, opening and dissemination of the 1,718 File was not authorized by LabMD.

124.

Defendant Tiversa took LabMD's personal property.

125.

Defendant Tiversa obtained LabMD's personal property by a deceitful means and artful practice.

126.

Defendant Tiversa used a computer and/or computer network with the intention of examining employment, medical, salary, credit, and other financial or personal data relating to third parties.



128.

Defendant Tiversa searched computer networks searching for, downloading, opening and dissemination LabMD computer files containing employment, medical, salary, credit, and other financial or personal data on numerous occasions.

129.

Defendant Johnson used a computer network to search for, download, open and disseminate the 1,718 File.

130.

Defendant Johnson knew that the searching for, downloading, opening and dissemination of the 1,718 File was not authorized by LabMD.

131.

Defendant Johnson took LabMD's personal property.

132.

Defendant Johnson obtained LabMD's personal property by a deceitful means and artful practice.

133.

Defendant Johnson used a computer and/or computer network with the intention of examining employment, medical, salary, credit, and other financial or personal data relating to third parties.

134.

Defendant Johnson searched computer networks searching for, downloading, opening and dissemination of LabMD computer files containing employment, medical, salary, credit, and other financial or personal data on numerous occasions.

135.

Defendants Tiversa and Johnson committed computer theft.

136.

Defendants Tiversa and Johnson committed computer invasion of privacy.

137.

As a result of Defendant Tiversa and Johnson's actions, LabMD has suffered damages in an amount to be proven at trial.

**COUNT III: CONVERSION**  
**(As to All Defendants)**

138.

LabMD realleges the allegations contained in Paragraphs 1 through 137 as though stated verbatim herein.

139.

The 1,718 File is owned by LabMD.

140.

Defendant Tiversa is in possession of the 1,718 File.

141.

Defendant Tiversa is not authorized to assume the right of ownership over the 1,718 File.

142.

The appropriation of the 1,718 File by Defendant Tiversa was not authorized by LabMD.

143.

Defendant Johnson is in possession of the 1,718 File.

144.

Defendant Johnson is not authorized to assume the right of ownership over the 1,718 File.

145.

The appropriation of the 1,718 File by Defendant Johnson was not authorized by LabMD.

146.

Defendant Dartmouth is in possession of the 1,718 File.

147.

Defendant Dartmouth is not authorized to assume the right of ownership over the 1,718 File.

148.

The appropriation of the 1,718 File by Defendant was not authorized by LabMD.

149.

LabMD informed Defendants that the 1,718 File belonged to LabMD. See Exhibits N, O and P.

150.

LabMD demanded return of the 1,718 File from Defendants.

151.

Defendants have not returned the 1,718 File to LabMD.

152.

As a result of Defendants' actions, LabMD has been damaged in an amount to be proven at trial.

**COUNT IV: TRESPASS**  
**(As to All Defendants)**

153.

LabMD realleges the allegations contained in Paragraphs 1 through 152 as though stated herein verbatim.

154.

Defendants have unlawfully abused LabMD's personal property.

155.

Defendants have damaged LabMD's personal property.

156.

As a result of Defendants' unlawful abuse of LabMD's personal property, LabMD has been damaged in an amount to be proven at trial.

**COUNT V: PUNITIVE DAMAGES**  
**(As to All Defendants)**

157.

LabMD realleges the allegations contained in Paragraph 1 through 156 as though stated herein verbatim.

158.

Defendants' actions described herein constitute willful misconduct, malice, fraud, wantonness and oppression.

159.

Defendants' actions herein constitute a want of care which would raise the presumption of a conscious indifference to consequences.

160.

LabMD is entitled to punitive damages from Defendants in an amount to be proven at trial.

WHEREFORE, LabMD prays for the following relief:

- (a) Judgment against Defendants as outlined herein;
- (b) Damages in an amount to be determined at trial;
- (c) Exemplary damages in an amount to be determined at trial.
- (d) Attorney's fees and costs associated with this litigation;
- (e) A trial by jury on the issues outlined herein;
- (f) All such other and further relief as the Court deems just and proper.

... 2 p 8

[SIGNATURE CONTINUE ON NEXT PAGE]

6 29 9

Respectfully submitted this 1 day of October, 2011.

---

Stephan P. Fusco  
Georgia Bar No. 281030  
LabMD, Inc.  
2030 Powers Ferry Road  
Building 500, Suite 520  
Atlanta, Georgia 30339  
Telephone: (678) 443-2343

*Attorney for Plaintiff LabMD, Inc.*

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

LABMD, INC.,	)	
	)	
Plaintiff,	)	
	)	Civil Action
v.	)	
	)	File No. 1:11-cv-04044-JOF
TIVERSA, INC., TRUSTEES OF	)	
DARTMOUTH COLLEGE, M.	)	
ERIC JOHNSON,	)	
Defendants.	)	

AFFIDAVIT OF SCOTT A. MOULTON

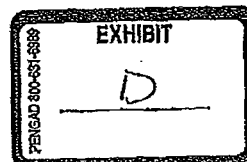
Personally appeared before the undersigned officer duly authorized to administer oaths, Scott A. Moulton, who after being duly sworn, deposes as follows:

1.

I am over 18 years of age, I am under no disability, and I am competent to give this affidavit. I give this affidavit of my own free will, and for use in the above-styled case, and for any other lawful purpose. The contents of this affidavit are based on my personal knowledge and my professional expertise.

2.

I am President of and Lead Certified Computer Forensic Specialist for Forensic Strategy Services, LLC. Since becoming involved in computer forensics,





I have developed extensive expertise in this area as well as provide training for police agencies all over the world on the specifics of forensics. I am a Certified Computer Forensic Specialist and have been in the industry of computer forensics for eleven years. I have been certified as a computer forensic specialist for nine years. My Curriculum Vitae is attached hereto as Exhibit "A."

3.

In order to discuss forensics and perform the duties of investigations and surveillance, the State of Georgia requires me to hold a Private Investigators License. I am a licensed Private Investigator in the State of Georgia as required.

4.

I have reviewed the Complaint and supporting exhibits filed in the above-referenced action. After reviewing Exhibit B to the Complaint, I learned that Defendants Tiversa and M. Eric Johnson, with Defendant Dartmouth's knowledge and consent, searched peer-to-peer ("P2P") networks and randomly gathered a sample of shared files related to health care and health care institutions. Defendant Tiversa's servers and software allowed Defendant Dartmouth and Defendant Johnson to sample for files in the four most popular P2P networks (each of which supports the most popular clients) including Gnutella, Aries and e-donkey. See Exhibit B to complaint, p.8.

5.

Through my work as a private investigator, I have examined P2P networks, including the Gnutella network. In my examination of the Gnutella P2P file sharing network, I have learned that computers on the Gnutella P2P network have software installed on them that facilitate the trading of computer files including images and videos. The software, when installed, allows the user to search for the pictures, movies, and other digital files by entering text as search terms. Some names of the software used include, but are not limited to, BearShare, LimeWire, Shareaza, Morpheus, Gnucleus, Phex and other software clients. Those software programs interface with the Gnutella Network and are called Gnutelliums and are simply user interfaces with the underlying network of other users.

6.

When a user makes a search request on the P2P Gnutella network, the search goes through an Ultra-peer and checks the listings on the computers connected to the Gnutella network. When a file is found that the user wants to download and a request for the file is made, the file comes directly from the Internet Protocol ("IP") address of the computer where the file is physically located because Ultra-peers only have the file listing and not the actual file.

7.

When a user seeks to download a file from the P2P Gnutella network, the P2P Gnutella network software program opens a Transmission Control Protocol / Internet Protocol ("TCP/IP") port at the site where the file is located.

8.

TCP/IP is a way of connecting to a host computer. In order to connect to a host computer, the computer seeking access to the host computer sends a command to the host computer to open a port at the host site and to transfer data from the host site.

9.

Opening a TCP/IP port to connect to a host computer at another location is the same as physically being at the host site to take action on the file.

10.

When Defendants Tiversa, Mr. Johnson and Dartmouth College searched for the May 13 File, they opened a physical TCP/IP connection on LabMD's computer located in the State of Georgia.

11.

Every computer file being shared on the Gnutella P2P network has a unique file signature called a Secure Hash Algorithm (SHA) version 1 ("SHA 1").

SHA 1 was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA). A SHA-1 value can be likened (in layman terms) to DNA. It is a mathematical fingerprint of a computer file that will remain the same for an unchanged file no matter where the file is found or on which computer the file is located. Changing the file name will not make a change to the actual digital file, nor will sending or trading the same file across the Internet change the digital signature.

12.

The Gnutella P2P network software clients that connect and share files calculate the SHA-1 values of the files in the user's shared folder upon start up of the software. The Gnutella Client Software makes the file names and those values available on the network.

13.

I have examined the computer file presented to LabMD from Defendant Tiversa on May 13, 2008 ("May 13 File"). The May 13 File has a unique SHA-1 value.

14.

If LabMD deleted the May 13 File, also known as the 1,718 File in LabMD's Complaint, from its computers, a person searching for the file will be unable to

locate a copy of the file because the P2P Gnutella network searches for files based upon the SHA-1 value.

15.


In connection with my forensic work on this matter, I have not found any evidence that the May 13 File exists on any other computer other than the LabMD computer where the file was saved.

16.

I hold all the foregoing opinions to a reasonable degree of certainty. All fees paid for my services are in no way contingent upon the results of my examination and report. I have no financial interest in the outcome of this action.

FURTHER AFFIANT SAITH NOT, this 12 day of Jan

2012.

  
SCOTT A. MOULTON

Sworn and subscribed before me  
This 12 day of Jan, 2012

  
NOTARY PUBLIC

My commission expires:

May 12, 2014

PATRICIA GILBRETH  
NOTARY PUBLIC  
FORSYTH COUNTY GEORGIA  
My Commission Expires  
May 12, 2014

Scott A. Moulton  
Forensic Strategy Services, LLC.  
601B Industrial Court  
Woodstock, Ga 30189  
Email: smoulton@ForensicStrategy.com

Phone: 770-926-5588  
Fax: 770-926-7089  
Cell: 770-402-0191  
Web: www.ForensicStrategy.com

### Scott A. Moulton

**Mr. Scott Moulton, CGFS: Certified Computer Forensic Specialist**

Mr. Moulton is president of Forensics Strategy Services, LLC. and began the company in 2000. Mr. Moulton is skilled in the areas of data recovery and system recovery including rebuilding Exchange servers and has spent the last seven years focusing on computer forensics.

#### Positions & Skills

**President, Forensic Strategy Services, LLC. Woodstock, GA (2000-Present)**  
**Forensic Data Recovery Litigation Support Expert, Private Detective**

- Handle complete forensic data collection and preparation of evidence where a personal computer contains data that may be useful in a legal case
- Developed and implemented a methodology when handling equipment and hard drives involved in forensic data recovery while maintaining the chain of custody
- Authored and published in magazines on the topic of computer forensics
- Skilled in rebuilding hard drives and forensic preservation of damaged drives
- Speaker on topic of data recovery and rebuilding hard drives and forensic topics
- Identification of internal security issues
- Georgia Employee Licensed Private Detective

**President, Network Installation Computer Services, Inc. Woodstock, GA (1993-Present)**  
**Senior Computer System Specialist**

- Technical Support for Data Recovery and Backup Protection
- Responsible for informing other staff of new methods for security and recovery
- Primary lead technician and system engineer

**Partner, Docupak Technologies, Inc. Kennesaw, GA (2001-Present)**  
**Forensic Developer**

- This team has a staff of web developers that has done projects for
- Georgia Pacific, Six Flags, etc.
- When a case that involves custom code or a specialized case that requires
- someone with experience in development, my status allows me to redirect
- employees from this company to help in forensic cases

**Time Plus, Inc. Marietta, GA (June 1990-1993)**  
**Networking and Accounting Support Consultant**

- Responsible for building and support of Novell Networks
- Responsible for support for all customer accounting servers using Solomon III/IV
- Development and code testing on project to Lockheed Martin

**Scott A. Moulton**  
**Forensic Strategy Services, LLC.**  
 601B Industrial Court  
 Woodstock, Ga 30189  
 Email: smoulton@ForensicStrategy.com

Phone: 770-926-5588  
 Fax: 770-926-7089  
 Cell: 770-402-0191  
 Web: www.ForensicStrategy.com

**Experience with Software and Hardware:**

- Forensic Imaging Specifications
- Experienced with Encase 4, 5 and 6
- Access Data FTK and Registry Tools
- Rebuilding Raid Arrays
- Expert in Data Recovery and Data Recovery Software, Runtime Software
- Expert in Rebuilding damaged Hard Drives
- Internal Windows System Recovery Formats
- Evidence Eliminator Software
- Hardware Write Blockers for Forensic Images with Tamper Resistant Processes
- CD Manufacturing and Data Recovery from CD's/DVD's
- RAID Array Systems and Recovery of Crashed RAID Systems
- Indexing and Search Software
- Most Hard Drives ever made, including assembly and disassembly of inner components
- Exchange Server, All Email Servers, Lotus Notes Email Servers
- Novell Operating Systems
- Microsoft Products Including but not limited to:
  - Microsoft Operating Systems
    - Windows 2003 Server
    - Windows 2003 Advanced Server
    - Windows NT Server
    - Exchange Server 2000 & 2003
  - ISA and Proxy Server and firewalls
  - Terminal Server and Advanced Terminal Server
  - Microsoft applications
- Internet and Web Applications
- Palm and Pocket PC System including the Data Recovery of both.
- Recovery of Photos and Pictures from Digital Camera and Digital Memory Sticks
- Recovery of all Firewire and USB Equipment
- Hardware and Software Sniffers, including Wireless
- Custom Written Tracking Systems and Monitoring Systems
- Firewalls both Hardware and Software
- Routers including Cisco, Ascend, Lucent
- Remote Application Software Including:
  - VPN, LAN, WAN
  - Web Sites
  - Web Applications
  - E-Commerce
- Windows Based Security Systems

**Memberships and Clubs:**

- Member of the Certified Fraud Examiners
- Woodstock Powercore Team Coordinator
- Toastmasters Cobb Micro Enterprises Kennesaw
- Interzone, LLC. Seminar Speaker
- GrayArea, LLC. Training Leader
- Defcon 404 Local Chapter
- Attending Defcon Las Vegas
- Electronic Frontier Foundation Member
- Licensed Encase 4 & 5 Investigator
- Licensed FTK Investigator

**Scott A. Moulton**  
**Forensic Strategy Services, L.L.C.**  
 601B Industrial Court  
 Woodstock, Ga 30189  
 Email: smoulton@ForensicStrategy.com

Phone: 770-926-5588  
 Fax: 770-926-7089  
 Cell: 770-102-0191  
 Web: www.ForensicStrategy.com

#### Certifications

- COFS: Certified Computer Forensic Specialist
- CCFT: Certified Computer Forensic Technician
- Georgia Employee Licensed Private Detective
- Aptec -- IOUC System Programmer and Developer Certified
- Microsoft Developer Network
- Microsoft Business Partner
- Lotus Business Partner
- Lotus Notes Developer
- Solomon III Accounting Server
- Solomon IV Accounting Server
- Solomon IV Accounting System Developer
- Novell Certified Network Administrator
- Trend Micro Security Solution Partner
- Dell Solution Provider

#### Education & Training

##### 1993 -- Present Training Events and Courses

- Taught Several Training Seminars on Computer Forensics, Computer Technology and Terminology, Application Usage and Presentation Formats
- Taught Forensics 101 Class to EarthLink's Fraud Department
- Completed Standard Computer Forensics & Electronic Discovery Training Course
- Completed Advanced Computer Forensics & Electronic Discovery Training Course
- Completed Lotus Notes Training Course
- Attended Training at Southeastern Cybercrime Summit.
- Forensic Training from Business Intelligence Associates
- "The Certified Fraud Examiner in Court"
- "Trends in Fraud Litigation"
- "Ethical Lessons for Financial Professionals"
- "Data Presentation" for Court sponsored by Certified Fraud Examiners
- "Best Practices for Data Protection and Recovery" by Winternals
- "Using Data Analysis Techniques to Find Fraud"
- "Data Retrieval and Data Protection" by David Benton, Georgia Bureau of Investigation

##### Attending:

1986 -- 1991 Southern College of Technology                      Marietta, Ga  
 Computer Science Major

- Campus Radio Announcer
- Computer consultant

1982 -- 1986 Benedictine Military Academy                      Savannah, Ga  
 College Preparatory With Distinction

- Savannah Stamp and Philatelic Society

#### Accomplishments

- Written and published in magazines on the topic of computer forensics
- Rebuilt hard drives and head assemblies successfully
- Attend All Certified Fraud Examiner meetings possible
- Participate in ACT Training Program as an Instructor for Internships
- Developed "Proof of Concept" Forensic Data Stripping Application
- Worked on application for F-22 for Lockheed under TimePlus
- Responsible for Reporting several bugs and fixes to Encase and Access Data teams



**Responses and Replies**1:11-cv-04044-JOF LabMD, Inc. v. Tiversa, Inc. et al

4months, STAY, SUBMDJ

**U.S. District Court****Northern District of Georgia****Notice of Electronic Filing**

The following transaction was entered by Fusco, Stephen on 1/13/2012 at 9:17 PM EST and filed on 1/13/2012

Case Name: LabMD, Inc. v. Tiversa, Inc. et al

Case Number: 1:11-cv-04044-JOF

Filer: LabMD, Inc.

Document Number: 17**Docket Text:**

RESPONSE in Opposition re [5] MOTION to Dismiss *Plaintiff's Complaint and Special Appearance* filed by LabMD, Inc.. (Attachments: # (1) Affidavit)(Fusco, Stephen)

1:11-cv-04044-JOF Notice has been electronically mailed to:

Andrew G. Phillips [aphillips@mcguirewoods.com](mailto:aphillips@mcguirewoods.com), [jhalvorson@mcguirewoods.com](mailto:jhalvorson@mcguirewoods.com),  
[mshuller@mcguirewoods.com](mailto:mshuller@mcguirewoods.com)

Jeffrey L. Mapen [jeff.mapen@nelsonmullins.com](mailto:jeff.mapen@nelsonmullins.com), [robin.dinning@nelsonmullins.com](mailto:robin.dinning@nelsonmullins.com)

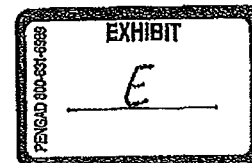
Richard Kennon Hines, V [richard.hines@nelsonmullins.com](mailto:richard.hines@nelsonmullins.com), [mandy.evangelista@nelsonmullins.com](mailto:mandy.evangelista@nelsonmullins.com),  
[maria.turner@nelsonmullins.com](mailto:maria.turner@nelsonmullins.com), [maureen.elliott@nelsonmullins.com](mailto:maureen.elliott@nelsonmullins.com)

Stephen Frank Fusco [sfusco@labmd.org](mailto:sfusco@labmd.org), [ksheriff@labmd.org](mailto:ksheriff@labmd.org)

1:11-cv-04044-JOF Notice has been delivered by other means to:

John C. Hansberry  
Pepper Hamilton-PA  
50th Floor, One Melton Bank Center  
500 Grant Street  
Pittsburgh, PA 15219

Richard M. Weibley  
Pepper Hamilton-PA  
50th Floor, One Melton Bank Center  
500 Grant Street  
Pittsburgh, PA 15219



1/13/2012 9:16 PM

The following document(s) are associated with this transaction:

**Document description:**Main Document

**Original filename:**n/a

**Electronic document Stamp:**

[STAMP dcecfStamp\_ID=1060868753 [Date=1/13/2012] [FileNumber=4849104-0]  
][69624d651526942ed6609f42d669096fc3adfa0919d4c8db74bb48dd563d3bc8e8a  
b97ae5b1d7dd9e019aae176b9e0974d295fb314df82cfe304a111aa750b5a]]

**Document description:**Affidavit

**Original filename:**n/a

**Electronic document Stamp:**

[STAMP dcecfStamp\_ID=1060868753 [Date=1/13/2012] [FileNumber=4849104-1]  
][23d7013ba025cff4f0d872acfc5a0cff37cafe287b9270f93b6f42e0a6e090e0865  
f2c34e106d512e0c85bc77a911cc9af69caf0f60be9e6ecfaf028969e6e9e]]

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

LABMD, INC.,	)	
	)	
Plaintiff,	)	CIVIL ACTION FILE NO.:
v.	)	1:11-CV-04044-JOF
	)	
TIVERSA, INC., TRUSTEES	)	
OF DARTMOUTH COLLEGE	)	
And M. ERIC JOHNSON,	)	
	)	
Defendants.	)	

---

LABMD'S RESPONSE TO DEFENDANT TIVERSA'S MOTION TO DISMISS

Comes now Plaintiff LabMD, Inc. ("LabMD" or "Plaintiff") and hereby files this response to Defendant Tiversa, Inc.'s ("Tiversa" or Defendant") Motion to Dismiss Plaintiff's Complaint ("Motion"):

INTRODUCTION

Defendant's request to dismiss Plaintiff's complaint trivializes the gravity of the situation by comparing the intentional downloading of highly sensitive, private medical information containing medical conditions of LabMD's patients to the simple downloading of music or client lists of a company. Defendant does not dispute that: (1) it intentionally searched computer networks fishing for sensitive computer files containing highly confidential personally identifiable health information ("PHI") and personally identifiable information ("PII"); (2) it downloaded computer files it knew contained PHI and PII; and (3) with

1. Defendant Tiversa's actions subject it to Georgia's Long Arm Statute.

Georgia's Long Arm Statute<sup>1</sup> provides that a court of this state may exercise personal jurisdiction over any nonresident if the person, among other things, commits a tortious act or omission within this state or commits a tortious injury in this state caused by an act or omission outside this state if the tort-feasor engages in certain conduct. O.C.G.A. § 9-10-91.

a. Defendant's actions constitute tortious acts within Georgia.

Defendant Tiversa is subject to this Honorable Court's jurisdiction if it "commits a tortious act or omission within" Georgia. O.C.G.A. 9-10-91 (2). While Defendant attempts to focus the inquiry on the physical location of the computer used to initiate its searches to argue that it did not commit a tortious act in the State of Georgia, such inquiry grossly oversimplifies P2P technology. While a user of P2P technology may be located in a remote location, P2P technology initiates certain actions at the location of the computer being searched and, as such, certain tortious acts take place at the site of the host computer. Therefore, so long as Defendant caused certain actions to be taken in Georgia, the physical location of Defendant is irrelevant.

Rather than offering a rudimentary layman's explanation of P2P

---

<sup>1</sup> While Defendant refers to O.C.G.A. §9-10-91(1), Plaintiff does not rely upon this. As such, Defendant's arguments related to O.C.G.A. 9-10-91(1) are moot.

technology<sup>2</sup>, Plaintiff relies upon the expertise of Scott A. Moulton. *See* Affidavit of Scott A. Moulton attached hereto as Exhibit A. Mr. Moulton's experience involves extensive research and knowledge regarding P2P technology. The Gnutella P2P network<sup>3</sup> is comprised of computers having software installed on them that facilitate the trading of computer files including images and videos. *See* Moulton Affidavit, ¶ 5. When a file is found that a user wants to download and a request for the file is made, the file comes directly from the Internet Protocol ("IP") address of the computer where the file is physically located. *Id.*

Once a user chooses to download a file from the P2P Gnutella network, the P2P Gnutella network software program opens a Transmission Control Protocol/ Internet Protocol ("TCP/IP") port at the site where the file is located by sending a command to the host computer to open a port at the host site and to transfer data from the host site.. *Id.* ¶¶ 7-8. Opening a TCP/IP port to connect to

---

<sup>2</sup> While Defendant relies upon Digiprotect USA Corporation v. John/Jane Does (2011 U.S. Dist. LEXIS 109464, \*8 (S.D.N.Y.C 2011)) the technology in question in that case focused on the swarming nature of the P2P network being searched. (Plaintiff's "argument is based on the nature of peer-to-peer networks in which unauthorized copies are distributed among peers. The mere fact that BitTorrent protocol and eDonkey network employ 'swarming' is insufficient to confer jurisdiction"). LabMD does not base its jurisdictional claim on the swarming technologies. Therefore, in addition to being precedent outside of this District Court, the basis of conferring jurisdiction on Defendant is totally different and is inapplicable in this case.

<sup>3</sup>It is undisputed that Defendant searched the Gnutella P2P network in 2009 searching for medical files containing PHI and PII. *See* Complaint, Exhibit B.



Bureau of Consumer Protection  
Division of Privacy and Identity Protection

United States of America  
FEDERAL TRADE COMMISSION  
WASHINGTON, DC 20530

October 24, 2013

VIA FEDERAL EXPRESS

Forensic Strategy Services LLC  
c/o Scott Moulton  
601B Industrial Court  
Woodstock, GA 30189-3529

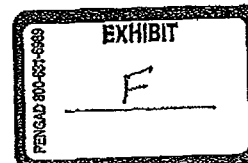
Re: In the Matter of LabMD, Inc., FTC Docket No. 9357

Dear Mr. Moulton:

The Commission recently initiated an adjudicative proceeding against LabMD, Inc. The Commission's Rules of Practice state that "[c]ounsel for a party may sign and issue a subpoena, on a form provided by the Secretary [of the Commission], commanding a person to produce and permit inspection and copying of designated books, documents, or tangible things. . . ." 16 C.F.R. § 3.34(b). This letter is to notify you that Complaint Counsel has issued a subpoena *duces tecum* for certain of Forensic Strategy Services LLC's documents. The subpoena and its schedule and exhibits are enclosed.

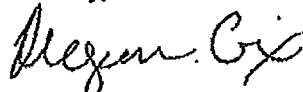
On August 29, 2013, the Federal Trade Commission's Office of Administrative Law Judges issued a Protective Order Governing Discovery Material (the "Protective Order") in the above-referenced action. The Protective Order protects confidential information produced in discovery in the case. A copy of the Protective Order signed by Chief Administrative Law Judge D. Michael Chappell is enclosed as an exhibit to the subpoena's schedule.

Any documents you produce to the Commission that are confidential must include the notice "CONFIDENTIAL - FTC Docket No. 9357," in accordance with paragraph 6 of the Protective Order. If you produce confidential documents in electronic format, such as on a CD or other media, you may place the "CONFIDENTIAL - FTC Docket No. 9357" designation on the CD.



I would be pleased to discuss any issues regarding production of documents at your earliest convenience. You may reach me at (202) 326-2282.

Sincerely,



Megan Cox

Enclosure (1)

cc: Michael Pepson (via email)  
Reed Rubinstein (via email)



## SUBPOENA DUCES TECUM

Provided by the Secretary of the Federal Trade Commission, and  
Issued Pursuant to Commission Rule 2.34(b), 16 C.F.R. § 3.34(b)(2010)

<b>1. TO</b>  Forensic Strategy Services LLC c/o Scott Moulton 601B Industrial Court Woodstock, GA 30189-3529	<b>2. FROM</b>  <p style="text-align: center;"><b>UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION</b></p>
<p style="text-align: center;">This subpoena requires you to produce and permit inspection and copying of designated books, documents (as defined in Rule 3.34(b)), or tangible things, at the date and time specified in Item 5, and at the request of Counsel listed in Item 9, in the proceeding described in Item 6.</p>	
<b>3. PLACE OF PRODUCTION</b>  Matthew Smith Federal Trade Commission 601 New Jersey Avenue, N.W. Room NJ-8100 Washington, D.C. 20001	<b>4. MATERIAL WILL BE PRODUCED TO</b>  Matthew Smith
<b>5. DATE AND TIME OF PRODUCTION</b>  November 21, 2013	
<b>6. SUBJECT OF PROCEEDING</b>  <p style="text-align: center;">In the Matter of LabMD, Inc., Docket 9357</p>	

<b>7. MATERIAL TO BE PRODUCED</b>  See attached Schedule and Exhibits, including the Protective Order Governing Discovery Material.	
<b>8. ADMINISTRATIVE LAW JUDGE</b>  Chief Judge D. Michael Chappell  Federal Trade Commission Washington, D.C. 20580	<b>9. COUNSEL AND PARTY ISSUING SUBPOENA</b>  Megan Cox, Complaint Counsel Federal Trade Commission 601 New Jersey Ave, N.W., Room NJ-8100 Washington, DC 20001 (202) 326-2282
<b>DATE SIGNED</b>  October 24, 2013	<b>SIGNATURE OF COUNSEL ISSUING SUBPOENA</b>  

### GENERAL INSTRUCTIONS

#### APPEARANCE

The delivery of this subpoena to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply.

#### MOTION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any motion to limit or quash this subpoena must comply with Commission Rule 3.34(e), 16 C.F.R. § 3.34(e), and in particular must be filed within the earlier of 10 days after service or the time for compliance. The original and ten copies of the motion must be filed before the Administrative Law Judge and with the Secretary of the Commission, accompanied by an affidavit of service of the document upon counsel listed in Item 9, and upon all other parties prescribed by the Rules of Practice.

#### TRAVEL EXPENSES

The Commission's Rules of Practice require that fees and mileage be paid by the party that requested your appearance. You should present your claim to counsel listed in Item 9 for payment. If you are permanently or temporarily living somewhere other than the address on this subpoena and it would require excessive travel for you to appear, you must get prior approval from counsel listed in Item 9.

A copy of the Commission's Rules of Practice is available online at <http://ftl.ftc.gov/FTCRulesofPractice>. Paper copies are available upon request.

This subpoena does not require approval by OMB under the Paperwork Reduction Act of 1980.



RETURN OF SERVICE

I hereby certify that a duplicate original of the within subpoena was duly served: (check the method used)

In person.

by registered mail.

by leaving copy at principal office or place of business, to wit:

Forensic Strategy Services LLC

601B Industrial Court

Woodstock, GA 30189-3529

*by Federal Express on October 24, 2013 for overnight delivery pursuant to Commission rule 44(a)(2)*

on the person named herein on:

October 26, 2013

(month, day, and year)

Matthew Smith

(name of person making service)

Paralegal

(Official title)

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

In the Matter of

LabMD, Inc.,  
a corporation

DOCKET NO. 9357

COMPLAINT COUNSEL'S SCHEDULE FOR  
PRODUCTION OF DOCUMENTS PURSUANT TO SUBPOENA TO  
FORENSIC STRATEGY SERVICES, LLC

Pursuant to Complaint Counsel's attached Subpoena Duces Tecum issued October 24, 2013, under Commission Rule of Practice § 3.34(b), Complaint Counsel requests that the following material be produced to the Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, DC 20001.

DEFINITIONS

1. "All documents" means each document, as defined below, that can be located, discovered or obtained by reasonable, diligent efforts, including without limitation all documents possessed by: (a) you, including documents stored in any personal electronic mail account, electronic device, or any other location under your control, or the control of your officers, employees, agents, or contractors; (b) your counsel; or (c) any other person or entity from which you can obtain such documents by request or which you have a legal right to bring within your possession by demand.
2. The term "Communication" includes, but is not limited to, any transmittal, exchange, transfer, or dissemination of information, regardless of the means by which it is accomplished, and includes all communications, whether written or oral, and all discussions, meetings, telephone communications, or email contacts.
3. "Company" shall mean Forensic Strategy Services, LLC, its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
4. "Complaint" means the Complaint issued by the Federal Trade Commission in the above-captioned matter on August 28, 2013.

5. The term "Containing" means containing, describing, or interpreting in whole or in part.
6. "Document" means the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including, but not limited to, any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, journal, agenda, minute, code book or label. "Document" shall also include electronically stored information ("ESI"). ESI means the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created or stored information, including, but not limited to, electronic mail, instant messaging, videoconferencing, and other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, thumb or flash drives, cell phones, Blackberry, PDA, or other storage media, and such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.
7. The term "Documents Sufficient to Show" means both documents that are necessary and documents that are sufficient to provide the specified information. If summaries, compilations, lists, or synopses are available that provide the information being requested, these may be provided in lieu of the underlying documents.
8. The terms "each," "any," and "all" shall be construed to have the broadest meaning whenever necessary to bring within the scope of any document request all documents that might otherwise be construed to be outside its scope.
9. "Includes" or "including" means "including, but not limited to," so as to avoid excluding any information that might otherwise be construed to be within the scope of any document request.
10. "LabMD" means LabMD, Inc., the named defendant in the above-captioned matter, and its directors, officers, employees and agents.
11. "Or" as well as "and" shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any document request all documents that otherwise might be construed to be outside the scope.
12. The term "Person" means any natural person, corporate entity, partnership, association, joint venture, governmental entity, or other legal entity.

13. "Personal Information" means individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.
14. The terms "Relate" or "Relating to" mean discussing, constituting, commenting, containing, concerning, embodying, summarizing, reflecting, explaining, describing, analyzing, identifying, stating, referring to, dealing with, or in any way pertaining to, in whole or in part.
15. "Subpoena" means the Subpoena to Forensic Strategy Services, LLC, including this Schedule and Exhibits, and including the Definitions, Instructions, and Specifications.
16. "You" or "Your" means Forensic Strategy Services, LLC, or the "Company."
17. The use of the singular includes the plural, and the plural includes the singular.
18. The use of a verb in any tense shall be construed as the use of the verb in all other tenses.

#### INSTRUCTIONS

1. **Applicable Time Period:** Unless otherwise specified, the time period covered by a document request shall be limited to the period from January 1, 2011 to present.
2. **Petitions to Limit or Quash:** Pursuant to Commission Rule of Practice § 3.34(c), any motion to limit or quash this subpoena must be filed within ten days of service thereof.
3. **Protective Order:** On August 29, 2013, the Court entered a Protective Order governing discovery material in this matter. A copy of the protective order is enclosed as Exhibit A, with instructions on the handling of confidential information.
4. **Document Identification:** Documents that may be responsive to more than one specification of this Subpoena need not be submitted more than once; however, the Company's response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this Subpoena have been previously supplied to the Commission, you may comply with this Subpoena by identifying the document(s) previously provided and the date of submission. Documents should be produced in the order in which they appear in your files or as electronically stored and without being manipulated or otherwise rearranged; if documents are removed from their original folders, binders, covers, containers, or electronic source in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, container, or electronic media or file paths from which such

documents came. In addition, number by page (or file, for those documents produced in native electronic format) all documents in your submission, preferably with a unique Bates identifier, and indicate the total number of documents in your submission.

5. **Production of Copies:** Unless otherwise stated, legible photocopies (or electronically rendered images or digital copies of native electronic files) may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this Subpoena. Further, copies of originals may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request. Copies of materials shall be produced in color if necessary to interpret them or render them intelligible.
6. **Sensitive Personally Identifiable Information:** If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please contact the Commission counsel named above before sending those materials to discuss ways to protect such information during production. For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
7. **Scope of Search:** These requests relate to documents that are in your possession or under your actual or constructive custody or control, including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, directors, officers, employees, or other agents or consultants, whether or not such documents were received from or disseminated to any other person or entity.
8. **Claims of Privilege:** Pursuant to the Federal Trade Commission's Rule of Practice 3.38A, 16 C.F.R. § 3.38A, if any documents are withheld from production based on a claim of privilege or any similar claim, you shall provide, not later than the date set for production of materials, a schedule that describes the nature of the documents, communications, or tangible things not produced or disclosed in a manner that will enable Complaint Counsel to assess the claim of privilege. The schedule shall state individually for each item withheld: (a) the document control number(s); (b) the full title (if the withheld material is a document) and the full file name (if the withheld material is in electronic form); (c) a description of the material withheld (for example, a letter,

memorandum, or email), including any attachments; (d) the date the material was created; (e) the date the material was sent to each recipient (if different from the date the material was created); (f) the email addresses, if any, or other electronic contact information to the extent used in the document, from which and to which each document was sent; (g) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all authors; (h) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all recipients of the material; (i) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all persons copied on the material; (j) the factual basis supporting the claim that the material is protected (for example, that it was prepared by an attorney rendering legal advice to a client in a confidential communication, or prepared by an attorney in anticipation of litigation regarding a specifically identified claim); and (k) any other pertinent information necessary to support the assertion of protected status by operation of law. If only part of a responsive document is privileged, all non-privileged portions of the document must be produced.

9. **Certification of Records of Regularly Conducted Activity:** Attached as Exhibit B is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena you to testify at future proceedings in order to establish the admissibility of documents produced in response to this subpoena. You are asked to execute this Certification and provide it with your response.
10. **Continuing Nature of Requests:** This request for documents shall be deemed continuing in nature so as to require production of all documents responsive to any specification included in this request produced or obtained by you prior to the close of discovery, which is March 5, 2014.
11. **Document Retention:** The Company shall retain all documentary materials used in the preparation of responses to the specifications of this Subpoena. We may require the submission of additional documents at a later time. Accordingly, the Company should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this litigation during its pendency, irrespective of whether the Company believes such documents are protected from discovery by privilege or otherwise.
12. **Electronic Submission of Documents:** The following guidelines refer to the production of any Electronically Stored Information ("ESI") or digitally imaged hard copy documents. Before submitting any electronic production, you must confirm with Commission counsel named above that the proposed formats and media types will be acceptable to the Commission. The FTC requests Concordance load-ready electronic productions, including DAT and OPT load files.
  - (1) **Electronically Stored Information:** Documents created, utilized, or maintained in electronic format in the ordinary course of business should be delivered to the FTC as follows:

- (a) Spreadsheet and presentation programs, including but not limited to Microsoft Access, SQL, and other databases, as well as Microsoft Excel and PowerPoint files, must be produced in native format with extracted text and metadata. Data compilations in Excel spreadsheets, or in delimited text formats, must contain all underlying data un-redacted with all underlying formulas and algorithms intact. All database productions (including structured data document systems) must include a database schema that defines the tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, Java, XML schemas, and other elements, including the use of any report writers and custom user data interfaces;
  - (b) All ESI other than those documents described in (1)(a) above must be provided in native electronic format with extracted text or Optical Character Recognition ("OCR") and all related metadata, and with corresponding image renderings as converted to Group IV, 300 DPI, single-page Tagged Image File Format ("TIFF") or as color JPEG images (where color is necessary to interpret the contents); and
  - (c) Each electronic file should be assigned a unique document identifier ("DocID") or Bates reference.
- (2) **Hard Copy Documents:** Documents stored in hard copy in the ordinary course of business should be submitted in an electronic format when at all possible. These documents should be true, correct, and complete copies of the original documents as converted to TIFF (or color JPEG) images with corresponding document-level OCR text. Such a production is subject to the following requirements:
- (a) Each page shall be endorsed with a document identification number (which can be a Bates number or a document control number); and
  - (b) Logical document determination should be clearly rendered in the accompanying load file and should correspond to that of the original document; and
  - (c) Documents shall be produced in color where necessary to interpret them or render them intelligible.
- (3) For each document electronically submitted to the FTC, you should include the following metadata fields in a standard ASCII delimited Concordance DAT file:
- (a) For electronic mail: begin Bates or unique document identification number ("DocID"), end Bates or DocID, mail folder path (location of email in personal folders, subfolders, deleted or sent items), custodian,

from, to, cc, bcc, subject, date and time sent, date and time received, and complete attachment identification, including the Bates or DocID of the attachments ("AttachIDs") delimited by a semicolon, MD5 or SHA Hash value, and link to native file;

- (b) For email attachments: begin Bates or DocID, end Bates or DocID, parent email ID (Bates or DocID), page count, custodian, source location/file path, file name, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file;
  - (c) For loose electronic documents (as retrieved directly from network file stores, hard drives, etc.): begin Bates or DocID, end Bates or DocID, page count, custodian, source media, file path, filename, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file; and
  - (d) For imaged hard-copy documents: begin Bates or DocID, end Bates or DocID, page count, source, and custodian; and where applicable, file folder name, binder name, attachment range, or other such references, as necessary to understand the context of the document as maintained in the ordinary course of business.
- (4) If you intend to utilize any de-duplication or email threading software or services when collecting or reviewing information that is stored in your computer systems or electronic storage media, or if your computer systems contain or utilize such software, you must contact the Commission counsel named above to determine whether and in what manner you may use such software or services when producing materials in response to this Subpoena.
- (5) Submit electronic productions as follows:
- (a) With passwords or other document-level encryption removed or otherwise provided to the FTC;
  - (b) As uncompressed electronic volumes on size-appropriate, Windows-compatible, media;
  - (c) All electronic media shall be scanned for and free of viruses;
  - (d) Data encryption tools may be employed to protect privileged or other personal or private information. The FTC accepts TrueCrypt, PGP, and SecureZip encrypted media. The passwords should be provided in advance of delivery, under separate cover. Alternate means of encryption should be discussed and approved by the FTC; and



- (e) Please mark the exterior of all packages containing electronic media sent through the U.S. Postal Service or other delivery services as follows:

**MAGNETIC MEDIA - DO NOT X-RAY  
MAY BE OPENED FOR POSTAL INSPECTION.**

- (6) All electronic files and images shall be accompanied by a production transmittal letter, which includes:
- (a) A summary of the number of records and all underlying images, emails, and associated attachments, native files, and databases in the production; and
  - (b) An index that identifies the corresponding consecutive document identification number(s) used to identify each person's documents and, if submitted in paper form, the box number containing such documents. If the index exists as a computer file(s), provide the index both as a printed hard copy and in machine-readable form (provided that the Commission counsel named above determines prior to submission that the machine-readable form would be in a format that allows the agency to use the computer files). The Commission counsel named above will provide a sample index upon request.

We have included a Bureau of Consumer Protection Production Guide as Exhibit C. This guide provides detailed directions on how to fully comply with this instruction.

13. **Documents No Longer In Existence:** If documents responsive to a particular specification no longer exist for reasons other than the ordinary course of business or the implementation of the Company's document retention policy but you have reason to believe have been in existence, state the circumstances under which they were lost or destroyed, describe the documents to the fullest extent possible, state the specification(s) to which they are responsive, and identify Persons having knowledge of the content of such documents.
14. **Incomplete Records:** If the Company is unable to answer any question fully, supply such information as is available. Explain why such answer is incomplete, the efforts made by the Company to obtain the information, and the source from which the complete answer may be obtained. If books and records that provide accurate answers are not available, enter best estimates and describe how the estimates were derived, including the sources or bases of such estimates. Estimated data should be followed by the notation "est." If there is no reasonable way for the Company to make an estimate, provide an explanation.
15. **Questions:** Any questions you have relating to the scope or meaning of anything in this request or suggestions for possible modifications thereto should be directed to Laura VanDruff, at (202) 326-2999, or Megan Cox, at (202) 326-2282. Documents responsive

to the request shall be addressed to the attention of Matthew Smith, Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, D.C. 20001, and delivered between 8:30 a.m. and 5:00 p.m. on any business day to the Federal Trade Commission.

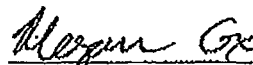
SPECIFICATIONS

Demand is hereby made for the following documents:

1. All communications between you and LabMD.
2. All documents considered to prepare the affidavit executed by Scott Moulton on January 12, 2012, in the matter captioned LabMD, Inc. v. Tiversa, Inc., Docket No. 11-cv-04044 (N.D. Ga.).
3. All contracts between you and LabMD.
4. All documents related to work you performed for LabMD.
5. All documents related to compensation received by you for services provided to LabMD.

October 24, 2013

By:



Alain Sheer  
Laura Riposo VanDruff  
Megan Cox  
Margaret Lassack  
Ryan Mehm

Complaint Counsel  
Bureau of Consumer Protection  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Room NJ-8100  
Washington, D.C. 20580  
Telephone: (202) 326-2282 (Cox)  
Facsimile: (202) 326-3062  
Electronic mail: [mcox1@ftc.gov](mailto:mcox1@ftc.gov)

CERTIFICATE OF SERVICE

This is to certify that on October 24, 2013, I served *via* electronic mail delivery a copy of the foregoing document to:

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

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

*Counsel for Respondent LabMD, Inc.*

October 24, 2013

By:



Matthew Smith  
Federal Trade Commission  
Bureau of Consumer Protection

# Exhibit A

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

In the Matter of

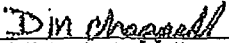
LabMD, Inc.,  
a corporation,  
Respondent.

DOCKET NO. 9357

PROTECTIVE ORDER GOVERNING DISCOVERY MATERIAL

Commission Rule 3.31(d) states: "In order to protect the parties and third parties against improper use and disclosure of confidential information, the Administrative Law Judge shall issue a protective order as set forth in the appendix to this section." 16 C.F.R. § 3.31(d). Pursuant to Commission Rule 3.31(d), the protective order set forth in the appendix to that section is attached verbatim as Attachment A and is hereby issued.

ORDERED:

  
\_\_\_\_\_  
D. Michael Chappell  
Chief Administrative Law Judge

Date: August 29, 2013

## ATTACHMENT A

For the purpose of protecting the interests of the parties and third parties in the above-captioned matter against improper use and disclosure of confidential information submitted or produced in connection with this matter:

**IT IS HEREBY ORDERED THAT** this Protective Order Governing Confidential Material ("Protective Order") shall govern the handling of all Discovery Material, as hereafter defined.

1. As used in this Order, "confidential material" shall refer to any document or portion thereof that contains privileged, competitively sensitive information, or sensitive personal information. "Sensitive personal information" shall refer to, but shall not be limited to, an individual's Social Security number, taxpayer identification number, financial account number, credit card or debit card number, driver's license number, state-issued identification number, passport number, date of birth (other than year), and any sensitive health information identifiable by individual, such as an individual's medical records. "Document" shall refer to any discoverable writing, recording, transcript of oral testimony, or electronically stored information in the possession of a party or a third party. "Commission" shall refer to the Federal Trade Commission ("FTC"), or any of its employees, agents, attorneys, and all other persons acting on its behalf, excluding persons retained as consultants or experts for purposes of this proceeding.
2. Any document or portion thereof submitted by a respondent or a third party during a Federal Trade Commission investigation or during the course of this proceeding that is entitled to confidentiality under the Federal Trade Commission Act, or any regulation, interpretation, or precedent concerning documents in the possession of the Commission, as well as any information taken from any portion of such document, shall be treated as confidential material for purposes of this Order. The identity of a third party submitting such confidential material shall also be treated as confidential material for the purposes of this Order where the submitter has requested such confidential treatment.
3. The parties and any third parties, in complying with informal discovery requests, disclosure requirements, or discovery demands in this proceeding may designate any responsive document or portion thereof as confidential material, including documents obtained by them from third parties pursuant to discovery or as otherwise obtained.
4. The parties, in conducting discovery from third parties, shall provide to each third party a copy of this Order so as to inform each such third party of his, her, or its rights herein.
5. A designation of confidentiality shall constitute a representation in good faith and after careful determination that the material is not reasonably believed to be already in the public domain and that counsel believes the material so designated constitutes confidential material as defined in Paragraph 1 of this Order.

6. Material may be designated as confidential by placing on or affixing to the document containing such material (in such manner as will not interfere with the legibility thereof), or if an entire folder or box of documents is confidential by placing or affixing to that folder or box, the designation "CONFIDENTIAL - FTC Docket No. 9357" or any other appropriate notice that identifies this proceeding, together with an indication of the portion or portions of the document considered to be confidential material. Confidential information contained in electronic documents may also be designated as confidential by placing the designation "CONFIDENTIAL - FTC Docket No. 9357" or any other appropriate notice that identifies this proceeding, on the face of the CD or DVD or other medium on which the document is produced. Masked or otherwise redacted copies of documents may be produced where the portions deleted contain privileged matter, provided that the copy produced shall indicate at the appropriate point that portions have been deleted and the reasons therefor.

7. Confidential material shall be disclosed only to: (a) the Administrative Law Judge presiding over this proceeding, personnel assisting the Administrative Law Judge, the Commission and its employees, and personnel retained by the Commission as experts or consultants for this proceeding; (b) judges and other court personnel of any court having jurisdiction over any appellate proceedings involving this matter; (c) outside counsel of record for any respondent, their associated attorneys and other employees of their law firm(s), provided they are not employees of a respondent; (d) anyone retained to assist outside counsel in the preparation or hearing of this proceeding including consultants, provided they are not affiliated in any way with a respondent and have signed an agreement to abide by the terms of the protective order; and (e) any witness or deponent who may have authored or received the information in question.

8. Disclosure of confidential material to any person described in Paragraph 7 of this Order shall be only for the purposes of the preparation and hearing of this proceeding, or any appeal therefrom, and for no other purpose whatsoever, provided, however, that the Commission may, subject to taking appropriate steps to preserve the confidentiality of such material, use or disclose confidential material as provided by its Rules of Practice; sections 6(f) and 21 of the Federal Trade Commission Act; or any other legal obligation imposed upon the Commission.

9. In the event that any confidential material is contained in any pleading, motion, exhibit or other paper filed or to be filed with the Secretary of the Commission, the Secretary shall be so informed by the Party filing such papers, and such papers shall be filed *in camera*. To the extent that such material was originally submitted by a third party, the party including the materials in its papers shall immediately notify the submitter of such inclusion. Confidential material contained in the papers shall continue to have *in camera* treatment until further order of the Administrative Law Judge, provided, however, that such papers may be furnished to persons or entities who may receive confidential material pursuant to Paragraphs 7 or 8. Upon or after filing any paper containing confidential material, the filing party shall file on the public record a duplicate copy of the paper that does not reveal confidential material. Further, if the protection for any such material expires, a party may file on the public record a duplicate copy which also contains the formerly protected material.



10. If counsel plans to introduce into evidence at the hearing any document or transcript containing confidential material produced by another party or by a third party, they shall provide advance notice to the other party or third party for purposes of allowing that party to seek an order that the document or transcript be granted *in camera* treatment. If that party wishes *in camera* treatment for the document or transcript, the party shall file an appropriate motion with the Administrative Law Judge within 5 days after it receives such notice. Except where such an order is granted, all documents and transcripts shall be part of the public record. Where *in camera* treatment is granted, a duplicate copy of such document or transcript with the confidential material deleted therefrom may be placed on the public record.

11. If any party receives a discovery request in any investigation or in any other proceeding or matter that may require the disclosure of confidential material submitted by another party or third party, the recipient of the discovery request shall promptly notify the submitter of receipt of such request. Unless a shorter time is mandated by an order of a court, such notification shall be in writing and be received by the submitter at least 10 business days before production, and shall include a copy of this Protective Order and a cover letter that will apprise the submitter of its rights hereunder. Nothing herein shall be construed as requiring the recipient of the discovery request or anyone else covered by this Order to challenge or appeal any order requiring production of confidential material, to subject itself to any penalties for non-compliance with any such order, or to seek any relief from the Administrative Law Judge or the Commission. The recipient shall not oppose the submitter's efforts to challenge the disclosure of confidential material. In addition, nothing herein shall limit the applicability of Rule 4.11(e) of the Commission's Rules of Practice, 16 CFR 4.11(e), to discovery requests in another proceeding that are directed to the Commission.

12. At the time that any consultant or other person retained to assist counsel in the preparation of this action concludes participation in the action, such person shall return to counsel all copies of documents or portions thereof designated confidential that are in the possession of such person, together with all notes, memoranda or other papers containing confidential information. At the conclusion of this proceeding, including the exhaustion of judicial review, the parties shall return documents obtained in this action to their submitters, provided, however, that the Commission's obligation to return documents shall be governed by the provisions of Rule 4.12 of the Rules of Practice, 16 CFR 4.12.

13. The provisions of this Protective Order, insofar as they restrict the communication and use of confidential discovery material, shall, without written permission of the submitter or further order of the Commission, continue to be binding after the conclusion of this proceeding.

# Exhibit B

**CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY**  
Pursuant to 28 U.S.C. § 1746

1. I, \_\_\_\_\_, have personal knowledge of the facts set forth below and am competent to testify as follows:
2. I have authority to certify the authenticity of the records produced by Forensic Strategy Services LLC and attached hereto.
3. The documents produced and attached hereto by Forensic Strategy Services LLC are originals or true copies of records of regularly conducted activity that:
  - a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
  - b) Were kept in the course of the regularly conducted activity of Forensic Strategy Services LLC; and
  - c) Were made by the regularly conducted activity as a regular practice of Forensic Strategy Services LLC.

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

Executed on \_\_\_\_\_, 2013.

\_\_\_\_\_  
Signature

---

# Exhibit C

---

**BCP PRODUCTION  
GUIDE**

As of 08/18/2011

## Bureau of Consumer Protection Production Guide

### An eDiscovery Resource

This guide explains what the Bureau of Consumer Protection (BCP) at the Federal Trade Commission (Commission) generally requires in response to a Civil Investigative Demand (CID) or a subpoena. The suggested formats are based on BCP's experience with many different submissions; follow them to organize your submission and minimize the chance of incompatibility with BCP's processes and systems.

This resource is intended as guidance and does not supersede instructions in any CID or subpoena. Please contact the Commission counsel identified in CID or subpoena to discuss any specific issues you may have with collecting, formatting, or submitting documents.

#### 1. Getting Started: Protocols for All Submissions

Before processing documents in response to a formal request, please note: The following protocols apply to ALL formats submitted to BCP. BCP has additional requirements pertaining to metadata, format, etc., for certain types of documents. See section 2 of these Instructions (entitled "Preparing Collections") for details.

##### a. Concordance Version and Load Files

BCP uses LexisNexis® Concordances® 2008 v 10.05. With the production, you must submit:

- an Opticon image load file (OPT) containing a line for every image file in the production, and
- a Concordance delimited data load file (DAT) containing a line for every document in the production, with Bates references, metadata fields, and native file links where applicable.

##### b. Virus Scanning

All electronic documents and production media shall be scanned and free of viruses prior to shipping to BCP. BCP will request replacement for any infected media, which may affect the timing of your compliance with BCP's request.

##### c. Extracted Text / OCR

Submit text:

- as document-level text files,
- named for the beginning Bates number, and
- organized into a folder separate from images.

*BCP cannot accept Unicode text files and will request replacement files if received.*

#### d. Deduplication

You must have the approval of Commission counsel to globally de-dupe or to apply email threading. You do not need prior approval of Commission counsel to deduplicate within a custodian's document set.

#### e. Labeling & Numbering Files

For image file names, bates numbers and document identification numbers (Doc IDs), use a consistent number of numerals to prevent issues with image display, using leading zeros where necessary. Do not use a space to separate the prefix from numbers.

Acceptable formats (as long as you are consistent)

- ABC-FTC0000001
- ABCFTC0000001

Unacceptable format

- ABC 0000001

#### f. Recommended Delimiters

BCP strongly recommends using these delimiters in delimited data load files:

Description	Symbol	ASCII Character
Field Separator	□	20
Quote Character	␣	254
Multi Entry delimiter	⊙	174
<Return> Value in data	~	126

#### g. Image Files

BCP only accepts image files that are:

- 300 DPI
- single-page Group IV TIFF files
- or color JPEG image files where color is necessary to interpret content

#### h. Date & Time Format

Submit date and time data in separate fields so Concordance can load it.

## 2. Preparing Collections

### a. Preparing Scanned Documents

Submit TIFF (or color JPEG) images with OCR text

### Metadata & Other Information Requirements

Include the following metadata fields and information in the delimited data load file. Alongside each piece of information, BCP recommends a corresponding field name for the delimited data load file.

<u>Document Info/ Metadata</u>	<u>Description</u>	<u>Concordance Field Name</u>
Beginning Bates number	The beginning bates number for the document	BEGBATES
Ending Bates number	The ending bates number for the document	ENDBATES
Page Count	The total number of pages in the document	PGCOUNT
Custodian	Mailbox where the email resided	CUSTODIAN

#### b. Preparing Email & Attachments

Email: Submit TIFF images with extracted text of email

#### Attachments:

- Submit Microsoft Excel and PowerPoint files in native format with extracted text and metadata.
- Submit Microsoft Access files and other multimedia files in native format with *metadata only*.
- Submit other files and attachments as images with extracted text and metadata.

#### Metadata & Other Information Requirements

- Preserve the parent/child relationship in email by including a reference to all attachments.
- Produce attachments as separate documents and number them consecutively to the parent email.
- Include the following metadata fields and information in the delimited data load file. Alongside each piece of information, BCP recommends a corresponding field name for the delimited data load file.

#### Metadata for Emails

<u>Document Info/ Metadata</u>	<u>Description</u>	<u>Concordance Field Name</u>
Beginning Bates number	The beginning bates number for the document	BEGBATES
Ending Bates number	The ending bates number for the document	ENDBATES
Page Count	The total number of pages in the document	PGCOUNT



Custodian	Mailbox where the email resided	CUSTODIAN
To	Recipient(s) of the email	RECIPIENT
From	The person who authored the email	FROM
CC	Person(s) copied on the email	CC
BCC	Person(s) blind copied on the email	BCC
Date Sent	Date the email was sent	DATESENT
Time Sent	Time the email was sent	TIMSENT
Subject	Subject line of email	SUBJECT
Date Received	Date the email was received	DATERCVD
Time Received	Time the email was received	TIMERCVD
Child records (attachments)	The beginning bates number(s) of attachments delimited by comma	ATTACHMENTID
Location or "Path"	Location of email in personal folders/Deleted Items/Sent Items	FILEPATH
Message ID	MS Outlook Message ID or similar number in other message systems	MESSAGEID

#### Metadata for Attachments

<u>Document Info / Metadata</u>	<u>Description</u>	<u>Concordance Field Name</u>
Beginning Bates number	The beginning bates number for the document	BEGBATBS
Ending Bates number	The ending bates number for the document	ENDBATBS
Page Count	The total number of pages in the document	PGCOUNT
Custodian	The name of the original custodian of the file	CUSTODIAN
Parent Record	Beginning bates number of parent email	PARENTID
Creation Date	The date attachment was saved at the location on the electronic media for the first time	CREBATE DATE
Creation Time	The time the attachment was saved at the location on the electronic media for the first time	CREBATE TIME
Modified Date	The date/time the attachment was last changed, and then saved	MODDATE
Modified Time	The time the attachment was last changed, and then saved	MODTIME
Last Accessed Date	The time the attachment was last opened, scanned, or even "touched" by a user or software activity	LASTACCDATE
Last Accessed Time	The time the attachment was last opened, scanned, or even "touched" by a user or software activity	LASTACCTIME

Size	The amount of space the file takes up on the electronic media. Usually recorded in kilobytes, however may be reported in single bytes	FILESIZE
File Name	The name of the attachment including the extension denoting the application in which the file was created	FILENAME
Native Link	Relative path of submitted native files such as Excel spreadsheets	NATIVELINK
Hash	The SHA (Secure Hash Algorithm) or MD5 (Message Digest) hash for the original native file if available	HASH

#### c. Preparing Native Files

- a. Submit Microsoft Access, Excel, and PowerPoint files in native format with extracted text and metadata.
- b. Submit other files and attachments as images with extracted text and metadata.

#### Metadata & Other Information Requirements

Include the following metadata fields and information in the delimited data load file. Alongside each piece of information, BCP recommends a corresponding field name for the delimited data load file.

#### Metadata and other information requirements for native files

Document Info / Metadata	Description	Correspondence Field Name
Beginning Bates number	The beginning bates number for the document	BEGBATES
Ending Bates number	The ending bates number for the document	ENDBATES
Page Count	The total number of pages in the document	PCCOUNT
Custodian	The name of the original custodian of the file	CUSTODIAN
Creation Date	The date attachment was saved at the location on the electronic media for the first time	CRBATEDATE
Creation Time	The time the attachment was saved at the location on the electronic media for the first time	CRBATE TIME
Modified Date	The date/time the attachment was last changed, and then saved	MODDATE
Modified Time	The time the attachment was last changed, and then saved	MOD TIME
Last Accessed Date	The time the attachment was last opened, scanned, or even "touched" by a user or software activity	LASTACCDATE
Last Accessed Time	The time the attachment was last opened, scanned, or even "touched" by a user or software activity	LASTACCTIME
Size	The amount of space the file takes up on the electronic media. Usually recorded in kilobytes	FILESIZE

File Name	The name of the file including the extension denoting the application in which the file was created	FILENAMB
Native link	Relative path of submitted native files	NATIVBLNK
Hash	The SHA (Secure Hash Algorithm) or MD5 Hash for the original native file if available	HASH

### 3. Submitting Your Production

Once you've prepared documents according to this guide, follow these instructions to submit them to BCP.

#### a. Media BCP Accepts

Submit any of the following:

- For Productions *under* 10 gigabytes:
  - CD-R CD-ROM optical disks formatted to ISO 9660 specifications
  - DVD-ROM optical disks for Windows-compatible personal computers
  - USB 2.0 flash drives
- For Productions *over* 10 gigabytes
  - IDE, EIDE and SATA hard disk drives, formatted in Windows-compatible, uncompressed data in a USB 2.0 external enclosure
  - USB 2.0 flash drives

#### b. Submit a Production Transmittal Letter

For any format, accompany the submission with a letter that includes all of the following:

- volume name,
- Bates ranges and custodians,
- total number of records,
- total number of images or files,
- list of fields in the order in which they are listed in the data files,
- date and time format, and
- confirmation that the number of files on the volume match the load files.



United States of America  
FEDERAL TRADE COMMISSION  
WASHINGTON, DC 20580

Bureau of Consumer Protection  
Division of Privacy and Identity Protection

November 27, 2013

VIA FEDERAL EXPRESS

Scott Moulton  
303 Eagle Ridge Place  
Canton, GA 30114

Re: In the Matter of LabMD, Inc., FTC Docket No. 9357

Dear Mr. Moulton:

Enclosed is a revised subpoena *ad testificandum* noticing your deposition for Thursday, February 6, 2014, the date on which you have agreed to make yourself available. We provided counsel for LabMD with notice of this date on Friday, November 22, 2013. They have not objected to our proceeding with your deposition on this date.

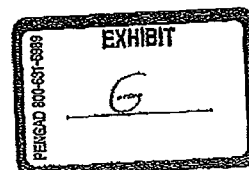
I would be pleased to discuss the scheduling of your deposition or other issues with you at your convenience. You may reach me at (202) 326-2999.

Sincerely,

Laura Riposo VanDruff

Enclosures (2)

cc: Michael Pepson (via email)  
Reed Rubinstein (via email)  
William A. Sherman, II (via email)





## SUBPOENA AD TESTIFICANDUM DEPOSITION

Provided by the Secretary of the Federal Trade Commission, and  
Issued Pursuant to Rule 3.34(a), 16 C.F.R. § 3.34(a) (2010)

<b>1. TO</b>  Scott Moulton 303 Eagle Ridge Place Canton, GA 30114	<b>2. FROM</b>  UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION
This subpoena requires you to appear and give testimony at the taking of a deposition, at the date and time specified in Item 6, and at the request of Counsel listed in Item 8, in the proceeding described in Item 6.	
<b>3. PLACE OF DEPOSITION</b>  Federal Trade Commission Southeast Region 225 Peachtree Street, NE, Suite 1600 Atlanta, GA 30303	<b>4. YOUR APPEARANCE WILL BE BEFORE</b>  Laura Riposo VanDruff or other designated counsel
<b>5. DATE AND TIME OF DEPOSITION</b>  February 6, 2014, at 9:00 a.m.	
<b>6. SUBJECT OF PROCEEDING</b>  In the Matter of LabMD, Inc., Docket 9357	
<b>7. ADMINISTRATIVE LAW JUDGE</b>  Chief Judge D. Michael Chappell  Federal Trade Commission Washington, D.C. 20580	<b>8. COUNSEL AND PARTY ISSUING SUBPOENA</b> Laura Riposo VanDruff, Complaint Counsel Federal Trade Commission 601 New Jersey Ave, NW, Room-8100 Washington, DC 20001 (202) 326-2099
<b>DATE SIGNED</b>  11/27/2013	<b>SIGNATURE OF COUNSEL ISSUING SUBPOENA</b>  

### GENERAL INSTRUCTIONS

#### APPEARANCE

The delivery of this subpoena to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply.

#### MOTION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any motion to limit or quash this subpoena must comply with Commission Rule 3.34(c), 16 C.F.R. § 3.34(c), and in particular must be filed within the earlier of 10 days after service or the time for compliance. The original and ten copies of the petition must be filed before the Administrative Law Judge and with the Secretary of the Commission, accompanied by an affidavit of service of the document upon counsel listed in Item 8, and upon all other parties prescribed by the Rules of Practice.

#### TRAVEL EXPENSES

The Commission's Rules of Practice require that fees and mileage be paid by the party that requested your appearance. You should present your claim to Counsel listed in Item 8 for payment. If you are permanently or temporarily living somewhere other than the address on this subpoena and it would require excessive travel for you to appear, you must get prior approval from Counsel listed in Item 8.

A copy of the Commission's Rules of Practice is available online at <http://ftc.gov/FTCRulesofPractice>. Paper copies are available upon request.

This subpoena does not require approval by OMB under the Paperwork Reduction Act of 1980.

**RETURN OF SERVICE**

*I hereby certify that a duplicate original of the within subpoena was duly served: (check the method used)*

- in person.*
- by registered mail* By Federal Express December 2, 2013 for overnight delivery pursuant to Commission rule 4.4(a)(2).
- by leaving copy at principal office or place of business, to wit:*

Scott Moulton  
303 Eagle Ridge Place  
Canton, GA 30114

*on the person named herein on:*  
November 28, 2013

*(month, day, and year)*

Matthew Smith

*(Name of person making service)*

Paralegal

*(Official title)*

CERTIFICATE OF SERVICE

This is to certify that on November 27, 2013, I served *via* electronic mail delivery a copy of the foregoing document to:

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

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

William A. Sherman, II  
Dinsmore & Shohl, LLP  
801 Pennsylvania Avenue, NW  
Suite 610  
Washington, D.C. 20004  
william.sherman@dinsmore.com

*Counsel for Respondent LabMD, Inc.*

November 27, 2013

By: 

Matthew Smith  
Federal Trade Commission  
Bureau of Consumer Protection

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

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

DOCKET NO. 9357

PROTECTIVE ORDER GOVERNING DISCOVERY MATERIAL

Commission Rule 3.31(d) states: "In order to protect the parties and third parties against improper use and disclosure of confidential information, the Administrative Law Judge shall issue a protective order as set forth in the appendix to this section," 16 C.F.R. § 3.31(d). Pursuant to Commission Rule 3.31(d), the protective order set forth in the appendix to that section is attached verbatim as Attachment A and is hereby issued.

ORDERED:

DM Chappell  
D. Michael Chappell  
Chief Administrative Law Judge

Date: August 29, 2013



## ATTACHMENT A

For the purpose of protecting the interests of the parties and third parties in the above-captioned matter against improper use and disclosure of confidential information submitted or produced in connection with this matter:

**IT IS HEREBY ORDERED THAT** this Protective Order Governing Confidential Material ("Protective Order") shall govern the handling of all Discovery Material, as hereafter defined.

1. As used in this Order, "confidential material" shall refer to any document or portion thereof that contains privileged, competitively sensitive information, or sensitive personnel information. "Sensitive personal information" shall refer to, but shall not be limited to, an individual's Social Security number, taxpayer identification number, financial account number, credit card or debit card number, driver's license number, state-issued identification number, passport number, date of birth (other than year), and any sensitive health information identifiable by individual, such as an individual's medical records. "Document" shall refer to any discoverable writing, recording, transcript of oral testimony, or electronically stored information in the possession of a party or a third party. "Commission" shall refer to the Federal Trade Commission ("FTC"), or any of its employees, agents, attorneys, and all other persons acting on its behalf, excluding persons retained as consultants or experts for purposes of this proceeding.
2. Any document or portion thereof submitted by a respondent or a third party during a Federal Trade Commission investigation or during the course of this proceeding that is entitled to confidentiality under the Federal Trade Commission Act, or any regulation, interpretation, or precedent concerning documents in the possession of the Commission, as well as any information taken from any portion of such document, shall be treated as confidential material for purposes of this Order. The identity of a third party submitting such confidential material shall also be treated as confidential material for the purposes of this Order where the submitter has requested such confidential treatment.
3. The parties and any third parties, in complying with informal discovery requests, disclosure requirements, or discovery demands in this proceeding may designate any responsive document or portion thereof as confidential material, including documents obtained by them from third parties pursuant to discovery or as otherwise obtained.
4. The parties, in conducting discovery from third parties, shall provide to each third party a copy of this Order so as to inform each such third party of his, her, or its rights herein.
5. A designation of confidentiality shall constitute a representation in good faith and after careful determination that the material is not reasonably believed to be already in the public domain and that counsel believes the material so designated constitutes confidential material as defined in Paragraph 1 of this Order.

6. Material may be designated as confidential by placing on or affixing to the document containing such material (in such manner as will not interfere with the legibility thereof), or if an entire folder or box of documents is confidential by placing or affixing to that folder or box, the designation "CONFIDENTIAL - FTC Docket No. 9357" or any other appropriate notice that identifies this proceeding, together with an indication of the portion or portions of the document considered to be confidential material. Confidential information contained in electronic documents may also be designated as confidential by placing the designation "CONFIDENTIAL - FTC Docket No. 9357" or any other appropriate notice that identifies this proceeding, on the face of the CD or DVD or other medium on which the document is produced. Masked or otherwise redacted copies of documents may be produced where the portions deleted contain privileged matter, provided that the copy produced shall indicate at the appropriate point that portions have been deleted and the reasons therefor.

7. Confidential material shall be disclosed only to: (a) the Administrative Law Judge presiding over this proceeding, personnel assisting the Administrative Law Judge, the Commission and its employees, and personnel retained by the Commission as experts or consultants for this proceeding; (b) judges and other court personnel of any court having jurisdiction over any appellate proceedings involving this matter; (c) outside counsel of record for any respondent, their associated attorneys and other employees of their law firm(s), provided they are not employees of a respondent; (d) anyone retained to assist outside counsel in the preparation or hearing of this proceeding including consultants, provided they are not affiliated in any way with a respondent and have signed an agreement to abide by the terms of the protective order; and (e) any witness or deponent who may have authored or received the information in question.

8. Disclosure of confidential material to any person described in Paragraph 7 of this Order shall be only for the purposes of the preparation and hearing of this proceeding, or any appeal therefrom, and for no other purpose whatsoever, provided, however, that the Commission may, subject to taking appropriate steps to preserve the confidentiality of such material, use or disclose confidential material as provided by its Rules of Practice; sections 6(f) and 21 of the Federal Trade Commission Act; or any other legal obligation imposed upon the Commission.

9. In the event that any confidential material is contained in any pleading, motion, exhibit or other paper filed or to be filed with the Secretary of the Commission, the Secretary shall be so informed by the Party filing such papers, and such papers shall be filed *in camera*. To the extent that such material was originally submitted by a third party, the party including the materials in its papers shall immediately notify the submitter of such inclusion. Confidential material contained in the papers shall continue to have *in camera* treatment until further order of the Administrative Law Judge, provided, however, that such papers may be furnished to persons or entities who may receive confidential material pursuant to Paragraphs 7 or 8. Upon or after filing any paper containing confidential material, the filing party shall file on the public record a duplicate copy of the paper that does not reveal confidential material. Further, if the protection for any such material expires, a party may file on the public record a duplicate copy which also contains the formerly protected material.

10. If counsel plans to introduce into evidence at the hearing any document or transcript containing confidential material produced by another party or by a third party, they shall provide advance notice to the other party or third party for purposes of allowing that party to seek an order that the document or transcript be granted *in camera* treatment. If that party wishes *in camera* treatment for the document or transcript, the party shall file an appropriate motion with the Administrative Law Judge within 5 days after it receives such notice. Except where such an order is granted, all documents and transcripts shall be part of the public record. Where *in camera* treatment is granted, a duplicate copy of such document or transcript with the confidential material deleted therefrom may be placed on the public record.

11. If any party receives a discovery request in any investigation or in any other proceeding or matter that may require the disclosure of confidential material submitted by another party or third party, the recipient of the discovery request shall promptly notify the submitter of receipt of such request. Unless a shorter time is mandated by an order of a court, such notification shall be in writing and be received by the submitter at least 10 business days before production, and shall include a copy of this Protective Order and a cover letter that will apprise the submitter of its rights hereunder. Nothing herein shall be construed as requiring the recipient of the discovery request or anyone else covered by this Order to challenge or appeal any order requiring production of confidential material, to subject itself to any penalties for non-compliance with any such order, or to seek any relief from the Administrative Law Judge or the Commission. The recipient shall not oppose the submitter's efforts to challenge the disclosure of confidential material. In addition, nothing herein shall limit the applicability of Rule 4.11(e) of the Commission's Rules of Practice, 16 CFR 4.11(e), to discovery requests in another proceeding that are directed to the Commission.

12. At the time that any consultant or other person retained to assist counsel in the preparation of this action concludes participation in the action, such person shall return to counsel all copies of documents or portions thereof designated confidential that are in the possession of such person, together with all notes, memoranda or other papers containing confidential information. At the conclusion of this proceeding, including the exhaustion of judicial review, the parties shall return documents obtained in this action to their submitters, provided, however, that the Commission's obligation to return documents shall be governed by the provisions of Rule 4.12 of the Rules of Practice, 16 CFR 4.12.

13. The provisions of this Protective Order, insofar as they restrict the communication and use of confidential discovery material, shall, without written permission of the submitter or further order of the Commission, continue to be binding after the conclusion of this proceeding.



## SUBPOENA DUCES TECUM

Provided by the Secretary of the Federal Trade Commission, and  
Issued Pursuant to Commission Rule 3.34(b), 16 C.F.R. § 3.34(b)(2010)

<b>1. TO</b>  Scott Moulton 303 Eagle Ridge Place Canton, GA 30114	<b>2. FROM</b>  UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION
--	--

This subpoena requires you to produce and permit inspection and copying of designated books, documents (as defined in Rule 3.34(b)), or tangible things, at the date and time specified in Item 5, and at the request of Counsel listed in Item 9, in the proceeding described in Item 6.

<b>3. PLACE OF PRODUCTION</b>  Matthew Smith Federal Trade Commission 601 New Jersey Avenue, N.W. Room NJ-8100 Washington, D.C. 20001	<b>4. MATERIAL WILL BE PRODUCED TO</b>  Matthew Smith
<b>5. DATE AND TIME OF PRODUCTION</b>  November 21, 2013	

<b>6. SUBJECT OF PROCEEDING</b>  <p style="text-align: center;">In the Matter of LabMD, Inc., Docket 9357</p>
---

<b>7. MATERIAL TO BE PRODUCED</b>  <p style="text-align: center;">See attached Schedule and Exhibits, including the Protective Order Governing Discovery Material.</p>
--

<b>8. ADMINISTRATIVE LAW JUDGE</b>  Chief Judge D. Michael Chappell  Federal Trade Commission Washington, D.C. 20580	<b>9. COUNSEL AND PARTY ISSUING SUBPOENA</b>  Megan Cox, Complaint Counsel Federal Trade Commission 601 New Jersey Ave, N.W., Room NJ-8100 Washington, DC 20001 (202) 326-2282
---	--

<b>DATE SIGNED</b>  October 24, 2013	<b>SIGNATURE OF COUNSEL ISSUING SUBPOENA</b>  
--	--

### GENERAL INSTRUCTIONS

#### APPEARANCE

The delivery of this subpoena to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply.

#### MOTION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any motion to limit or quash this subpoena must comply with Commission Rule 3.34(c), 16 C.F.R. § 3.34(c), and in particular must be filed within the earlier of 10 days after service or the time for compliance. The original and ten copies of the petition must be filed before the Administrative Law Judge and with the Secretary of the Commission, accompanied by an affidavit of service of the document upon counsel listed in Item 9, and upon all other parties prescribed by the Rules of Practice.

#### TRAVEL EXPENSES

The Commission's Rules of Practice require that fees and mileage be paid by the party that requested your appearance. You should present your claim to counsel listed in Item 9 for payment. If you are permanently or temporarily living somewhere other than the address on this subpoena and it would require excessive travel for you to appear, you must get prior approval from counsel listed in Item 9.

A copy of the Commission's Rules of Practice is available online at <http://bit.ly/FTCRulesofPractice>. Paper copies are available upon request.

This subpoena does not require approval by OMB under the Paperwork Reduction Act of 1980.

RETURN OF SERVICE

I hereby certify that a duplicate original of the within subpoena was duly served: (check the method used)

in person.

by registered mail - by Federal Express on October 24, 2013 for overnight delivery, pursuant to  
Court Order rule 4.4(a)(2)

by leaving copy at principal office or place of business, to wit:

Scott Moulton

303 Eagle Ridge Place

Canton, GA 30114

on the person named herein on:

October 25, 2013

(Month, day, and year)

Matthew Smith

(Name of person making service)

Paralegal

(Official title)

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

In the Matter of

LabMD, Inc.,  
a corporation

DOCKET NO. 9357

COMPLAINT COUNSEL'S SCHEDULE FOR  
PRODUCTION OF DOCUMENTS PURSUANT TO SUBPOENA TO  
SCOTT MOULTON

Pursuant to Complaint Counsel's attached Subpoena Duces Tecum issued October 24, 2013, under Commission Rule of Practice § 3.34(b), Complaint Counsel requests that the following material be produced to the Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, DC 20001.

DEFINITIONS

1. "All documents" means each document, as defined below, that can be located, discovered or obtained by reasonable, diligent efforts, including without limitation all documents possessed by: (a) you, including documents stored in any personal electronic mail account, electronic device, or any other location under your control, or the control of your officers, employees, agents, or contractors; (b) your counsel; or (c) any other person or entity from which you can obtain such documents by request or which you have a legal right to bring within your possession by demand.
2. The term "Communication" includes, but is not limited to, any transmittal, exchange, transfer, or dissemination of information, regardless of the means by which it is accomplished, and includes all communications, whether written or oral, and all discussions, meetings, telephone communications, or email contacts.
3. "Complaint" means the Complaint issued by the Federal Trade Commission in the above-captioned matter on August 28, 2013.
4. The term "Containing" means containing, describing, or interpreting in whole or in part.
5. "Document" means the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or

location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including, but not limited to, any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, journal, agenda, minute, code book or label. "Document" shall also include electronically stored information ("ESI"). ESI means the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created or stored information, including, but not limited to, electronic mail, instant messaging, videoconferencing, and other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, thumb or flash drives, cell phones, Blackberry, PDA, or other storage media, and such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.

6. The terms "each," "any," and "all" shall be construed to have the broadest meaning whenever necessary to bring within the scope of any document request all documents that might otherwise be construed to be outside its scope.
7. "Includes" or "including" means "including, but not limited to," so as to avoid excluding any information that might otherwise be construed to be within the scope of any document request.
8. "LabMD" means LabMD, Inc., the named defendant in the above-captioned matter, and its directors, officers, employees and agents.
9. "Or" as well as "and" shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any document request all documents that otherwise might be construed to be outside the scope.
10. The term "Person" means any natural person, corporate entity, partnership, association, joint venture, governmental entity, or other legal entity.
11. "Personal Information" means individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.
12. The terms "Relate" or "Relating to" mean discussing, constituting, commenting, containing, concerning, embodying, summarizing, reflecting, explaining, describing,

analyzing, identifying, stating, referring to, dealing with, or in any way pertaining to, in whole or in part.

13. "Subpoena" means the Subpoena to Scott Moulton, including this Schedule and Exhibits, and including the Definitions, Instructions, and Specifications.
14. "You" or "Your" means Scott Moulton.
15. The use of the singular includes the plural, and the plural includes the singular.
16. The use of a verb in any tense shall be construed as the use of the verb in all other tenses.

#### INSTRUCTIONS

1. **Applicable Time Period:** Unless otherwise specified, the time period covered by a document request shall be limited to the period from **January 1, 2011 to present**.
2. **Petitions to Limit or Quash:** Pursuant to Commission Rule of Practice § 3.34(c), any motion to limit or quash this subpoena must be filed within ten days of service thereof.
3. **Protective Order:** On August 29, 2013, the Court entered a Protective Order governing discovery material in this matter. A copy of the protective order is enclosed as Exhibit A, with instructions on the handling of confidential information.
4. **Document Identification:** Documents that may be responsive to more than one specification of this Subpoena need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this Subpoena have been previously supplied to the Commission, you may comply with this Subpoena by identifying the document(s) previously provided and the date of submission. Documents should be produced in the order in which they appear in your files or as electronically stored and without being manipulated or otherwise rearranged; if documents are removed from their original folders, binders, covers, containers, or electronic source in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, container, or electronic media or file paths from which such documents came. In addition, number by page (or file, for those documents produced in native electronic format) all documents in your submission, preferably with a unique Bates identifier, and indicate the total number of documents in your submission.
5. **Production of Copies:** Unless otherwise stated, legible photocopies (or electronically rendered images or digital copies of native electronic files) may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this Subpoena. Further, copies of originals may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in



any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request. Copies of materials shall be produced in color if necessary to interpret them or render them intelligible.

6. **Sensitive Personally Identifiable Information:** If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please contact the Commission counsel named above before sending those materials to discuss ways to protect such information during production. For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
7. **Scope of Search:** These requests relate to documents that are in your possession or under your actual or constructive custody or control, including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, directors, officers, employees, or other agents or consultants, whether or not such documents were received from or disseminated to any other person or entity.
8. **Claims of Privilege:** Pursuant to the Federal Trade Commission's Rule of Practice 3.38A, 16 C.F.R. § 3.38A, if any documents are withheld from production based on a claim of privilege or any similar claim, you shall provide, not later than the date set for production of materials, a schedule that describes the nature of the documents, communications, or tangible things not produced or disclosed in a manner that will enable Complaint Counsel to assess the claim of privilege. The schedule shall state individually for each item withheld: (a) the document control number(s); (b) the full title (if the withheld material is a document) and the full file name (if the withheld material is in electronic form); (c) a description of the material withheld (for example, a letter, memorandum, or email), including any attachments; (d) the date the material was created; (e) the date the material was sent to each recipient (if different from the date the material was created); (f) the email addresses, if any, or other electronic contact information to the extent used in the document, from which and to which each document was sent; (g) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all authors; (h) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all recipients of the material; (i) the names, titles, business addresses, email addresses or other electronic contact information, and relevant affiliations of all persons copied on the material; (j) the factual basis supporting the claim that the material is protected (for example, that it was prepared by an attorney rendering legal advice to a client in a

confidential communication, or prepared by an attorney in anticipation of litigation regarding a specifically identified claim); and (k) any other pertinent information necessary to support the assertion of protected status by operation of law. If only part of a responsive document is privileged, all non-privileged portions of the document must be produced.

9. **Certification of Records of Regularly Conducted Activity:** Attached as Exhibit B is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena you to testify at future proceedings in order to establish the admissibility of documents produced in response to this subpoena. You are asked to execute this Certification and provide it with your response.
10. **Continuing Nature of Requests:** This request for documents shall be deemed continuing in nature so as to require production of all documents responsive to any specification included in this request produced or obtained by you prior to the close of discovery, which is March 5, 2014.
11. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this Subpoena. We may require the submission of additional documents at a later time. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this litigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise.
12. **Electronic Submission of Documents:** The following guidelines refer to the production of any Electronically Stored Information ("ESI") or digitally imaged hard copy documents. Before submitting any electronic production, you must confirm with Commission counsel named above that the proposed formats and media types will be acceptable to the Commission. The FTC requests Concordance load-ready electronic productions, including DAT and OPT load files.
  - (1) **Electronically Stored Information:** Documents created, utilized, or maintained in electronic format in the ordinary course of business should be delivered to the FTC as follows:
    - (a) Spreadsheet and presentation programs, including but not limited to Microsoft Access, SQL, and other databases, as well as Microsoft Excel and PowerPoint files, must be produced in native format with extracted text and metadata. Data compilations in Excel spreadsheets, or in delimited text formats, must contain all underlying data un-redacted with all underlying formulas and algorithms intact. All database productions (including structured data document systems) must include a database schema that defines the tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links,

directories, Java, XML schemas, and other elements, including the use of any report writers and custom user data interfaces;

- (b) All ESI other than those documents described in (1)(a) above must be provided in native electronic format with extracted text or Optical Character Recognition ("OCR") and all related metadata, and with corresponding image renderings as converted to Group IV, 300 DPI, single-page Tagged Image File Format ("TIFF") or as color JPEG images (where color is necessary to interpret the contents); and
- (c) Each electronic file should be assigned a unique document identifier ("DocID") or Bates reference.

(2) **Hard Copy Documents:** Documents stored in hard copy in the ordinary course of business should be submitted in an electronic format when at all possible. These documents should be true, correct, and complete copies of the original documents as converted to TIFF (or color JPEG) images with corresponding document-level OCR text. Such a production is subject to the following requirements:

- (a) Each page shall be endorsed with a document identification number (which can be a Bates number or a document control number); and
- (b) Logical document determination should be clearly rendered in the accompanying load file and should correspond to that of the original document; and
- (c) Documents shall be produced in color where necessary to interpret them or render them intelligible.

(3) For each document electronically submitted to the FTC, you should include the following metadata fields in a standard ASCII delimited Concordance DAT file:

- (a) For electronic mail: begin Bates or unique document identification number ("DocID"), end Bates or DocID, mail folder path (location of email in personal folders, subfolders, deleted or sent items), custodian, from, to, cc, bcc, subject, date and time sent, date and time received, and complete attachment identification, including the Bates or DocID of the attachments ("AttachIDs") delimited by a semicolon, MD5 or SHA Hash value, and link to native file;
- (b) For email attachments: begin Bates or DocID, end Bates or DocID, parent email ID (Bates or DocID), page count, custodian, source location/file path, file name, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file;

- (c) For loose electronic documents (as retrieved directly from network file stores, hard drives, etc.): begin Bates or DocID, end Bates or DocID, page count, custodian, source media, file path, filename, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file; and
  - (d) For imaged hard-copy documents: begin Bates or DocID, end Bates or DocID, page count, source, and custodian; and where applicable, file folder name, binder name, attachment range, or other such references, as necessary to understand the context of the document as maintained in the ordinary course of business.
- (4) If you intend to utilize any de-duplication or email threading software or services when collecting or reviewing information that is stored in your computer systems or electronic storage media, or if your computer systems contain or utilize such software, you must contact the Commission counsel named above to determine whether and in what manner you may use such software or services when producing materials in response to this Subpoena.
- (5) Submit electronic productions as follows:
- (a) With passwords or other document-level encryption removed or otherwise provided to the FTC;
  - (b) As uncompressed electronic volumes on size-appropriate, Windows-compatible, media;
  - (c) All electronic media shall be scanned for and free of viruses;
  - (d) Data encryption tools may be employed to protect privileged or other personal or private information. The FTC accepts TrueCrypt, PGP, and SecureZip encrypted media. The passwords should be provided in advance of delivery, under separate cover. Alternate means of encryption should be discussed and approved by the FTC; and
  - (e) Please mark the exterior of all packages containing electronic media sent through the U.S. Postal Service or other delivery services as follows:  
  
**MAGNETIC MEDIA – DO NOT X-RAY  
MAY BE OPENED FOR POSTAL INSPECTION.**
- (6) All electronic files and images shall be accompanied by a production transmittal letter, which includes:
- (a) A summary of the number of records and all underlying

images, emails, and associated attachments, native files, and databases in the production; and

- (b) An index that identifies the corresponding consecutive document identification number(s) used to identify each person's documents and, if submitted in paper form, the box number containing such documents. If the index exists as a computer file(s), provide the index both as a printed hard copy and in machine-readable form (provided that the Commission counsel named above determines prior to submission that the machine-readable form would be in a format that allows the agency to use the computer files). The Commission counsel named above will provide a sample index upon request.

We have included a Bureau of Consumer Protection Production Guide as Exhibit C. This guide provides detailed directions on how to fully comply with this instruction.

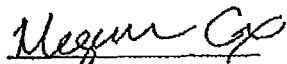
13. **Documents No Longer In Existence:** If documents responsive to a particular specification no longer exist for reasons other than the ordinary course of business or the implementation of a document retention policy but you have reason to believe have been in existence, state the circumstances under which they were lost or destroyed, describe the documents to the fullest extent possible, state the specification(s) to which they are responsive, and identify Persons having knowledge of the content of such documents.
14. **Incomplete Records:** If you are unable to answer any question fully, supply such information as is available. Explain why such answer is incomplete, the efforts made by you to obtain the information, and the source from which the complete answer may be obtained. If books and records that provide accurate answers are not available, enter best estimates and describe how the estimates were derived, including the sources or bases of such estimates. Estimated data should be followed by the notation "est." If there is no reasonable way for you to make an estimate, provide an explanation.
15. **Questions:** Any questions you have relating to the scope or meaning of anything in this request or suggestions for possible modifications thereto should be directed to Laura VanDruff, at (202) 326-2999, or Megan Cox, at (202) 326-2282. Documents responsive to the request shall be addressed to the attention of Matthew Smith, Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, D.C. 20001, and delivered between 8:30 a.m. and 5:00 p.m. on any business day to the Federal Trade Commission.

SPECIFICATIONS

Demand is hereby made for the following documents:

1. All communications between you and LabMD.
2. All documents considered to prepare the affidavit you executed on January 12, 2012, in the matter captioned LabMD, Inc. v. Tiversa, Inc., Docket No. 11-cv-04044 (N.D. Ga.).
3. All contracts between you and LabMD.
4. All documents related to work you performed for LabMD.
5. All documents related to compensation received by you, Forensic Strategy Services, LLC, or any other entity, for services you provided to LabMD.

October 24, 2013

By:   
Alain Sheer  
Laura Riposo VanDruff  
Megan Cox  
Margaret Lassack  
Ryan Mehrn

Complaint Counsel  
Bureau of Consumer Protection  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Room NJ-8100  
Washington, D.C. 20580  
Telephone: (202) 326-2282 (Cox)  
Facsimile: (202) 326-3062  
Electronic mail: [mcox1@ftc.gov](mailto:mcox1@ftc.gov)

CERTIFICATE OF SERVICE

This is to certify that on October 24, 2013, I served *via* electronic mail delivery a copy of the foregoing document to:

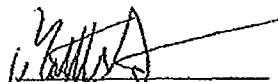
Michael D. Pepson  
Regulatory Counsel  
Cause of Action  
1919 Pennsylvania Avenue, NW, Suite 650  
Washington, D.C. 20006  
michael.pepson@causeofaction.org

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

*Counsel for Respondent LabMD, Inc.*

October 24, 2013

By:



Matthew Smith  
Federal Trade Commission  
Bureau of Consumer Protection


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

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

**STATEMENT PURSUANT TO SCHEDULING ORDER**

Pursuant to the Additional Provisions set forth in paragraph 4 of the Scheduling Order, Counsel for the moving party, Forensic Strategy Services, LLC, and Scott Moulton, hereby certifies that counsel met and conferred with Complaint Counsel via teleconference in a good-faith effort to resolve by agreement the issues set forth in Third-Party Forensic Strategy Services, LLC's Motion for Protective Order Regarding Complaint Counsel's Subpoena *Ad Testificandum* and Subpoena *Duces Tecum*, but the parties were unable to reach agreement. The required conference occurred on Monday, December 9, 2013, at approximately 10 a.m. between undersigned counsel and Alain Sheer, Ryan Mehm, Laura Riposo VanDuff and one additional attorney and a paralegal from Complaint Counsel's office.

Respectfully submitted,

  
\_\_\_\_\_  
Elizabeth G. Howard  
Georgia Bar No. 100118  
Barrickman, Allred & Young, LLC  
5775 Glenridge Drive, NE, Suite E-100  
Atlanta, GA 30328  
Telephone: (404) 252-2230  
Fax: (404) 252-3376  
[egh@bayatl.com](mailto:egh@bayatl.com)

Dated: 12/11/13



**CERTIFICATE OF SERVICE**

I hereby certify that on December 11, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

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

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

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

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

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

Michael D. Pepson  
Cause of Action  
1919 Pennsylvania Ave., NW, Suite 650  
Washington, D.C. 20006  
Phone: 202.499.4232  
Email: michael.pepson@causeofaction.org

**CERTIFICATE OF ELECTRONIC FILING**

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

Dated: December 11, 2013

By: 

Elizabeth G. Howard  
Georgia Bar No. 100118  
Barrickman, Allred & Young, LLC  
5775 Glenridge Drive, NE, Suite E-100  
Atlanta, GA 30328  
Telephone: (404) 252-2230  
Fax: (404) 252-3376  
[egh@bayatl.com](mailto:egh@bayatl.com)