

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

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

AUG 29 2012

JAMES N. HATTEN, Clerk
By: *[Signature]*
HARRY CLARK

FEDERAL TRADE
COMMISSION,

Petitioner,

v.

LABMD, INC., and

MICHAEL J. DAUGHERTY,

Respondents.

Misc. No. _____

1:12-CV-3005

WSD

**PETITION OF THE FEDERAL TRADE COMMISSION FOR AN ORDER
TO ENFORCE CIVIL INVESTIGATIVE DEMANDS**

Petitioner, the Federal Trade Commission ("FTC" or "Commission") petitions this Court, pursuant to Sections 16 and 20 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 56 and 57b-1, 28 U.S.C. §§ 1337 and 1345, and Fed. R. Civ. P. 81(a)(5), for an order requiring respondents, LabMD, Inc. ("LabMD") and Michael J. Daugherty, to comply with Civil Investigative Demands ("CID"), a type of administrative compulsory process, issued to respondents on December 21, 2011. The CIDs direct LabMD and Mr. Daugherty

to appear for testimony and to respond to interrogatories, require LabMD to produce documents in response to a document request, and instruct both respondents to provide a sworn verification as to these responses. The CIDs were issued in the course of a non-public investigation concerning possible violations by respondents of Section 5 of the FTC Act, 15 U.S.C. § 45(a), with respect to unfair or deceptive acts or practices involving consumer privacy and/or data security.

The Declaration under penalty of perjury of Alain Sheer, which verifies the allegations of this Petition, is attached hereto as Petition Exhibit 1.

In support of its Petition, the Commission alleges as follows:

1. The Commission is an administrative agency of the United States, organized and existing pursuant to the FTC Act, 15 U.S.C. § 41 *et seq.* The Commission is authorized by Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), to prohibit, *inter alia*, “unfair or deceptive acts or practices in or affecting commerce.”

2. In order to determine whether violations of Section 5 may have occurred, Section 3 of the FTC Act, 15 U.S.C. § 43, empowers the Commission to prosecute any inquiry necessary to its duties in any part of the United States. Section 6 of the Act, 15 U.S.C. § 46, empowers the Commission to gather and compile information concerning, and to investigate from time to time, the business

and practices of persons, partnerships or corporations engaged in or whose business affects commerce, with certain exceptions not relevant here; and Section 20 of the FTC Act, 15 U.S.C. § 57b-1, empowers the Commission to issue CIDs to require any person, *inter alia*, to produce documentary material, to file written reports or answers, and to give oral testimony relating to any Commission law enforcement investigation.

3. This Court has jurisdiction over respondents and the authority to enforce the CIDs pursuant to Section 20(e) of the FTC Act, which provides, in pertinent part as follows:

Whenever any person fails to comply with any civil investigative demand duly served upon him under this section, or whenever satisfactory copying or reproduction of material requested pursuant to the demand cannot be accomplished and such person refuses to surrender such material, the Commission, through such officers or attorneys as it may designate, may file, in the district court of the United States for any judicial district in which such person resides, is found, or transacts business, and serve upon such person, a petition for an order of such court for the enforcement of this section.

15 U.S.C. § 57b-1(e).

4. Respondent LabMD, Inc., is a Georgia corporation located at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia, 30339. It performs medical testing services for patients in Georgia and other parts of the United States.

Pet. Exh. 1 ¶ 3. Respondent Michael J. Daugherty is the owner and president of LabMD. Pet. Exh. 1 ¶ 1. Respondents engage in commerce throughout the country, including in this district, as the term “commerce” is defined in Section 4 of the FTC Act. 15 U.S.C. § 44. As respondents have engaged in commerce in this district, and maintain documents and information responsive to the CIDs within this district, the Northern District of Georgia is a jurisdiction within which respondents “reside, [are] found, or transact[] business” Thus, venue is proper under Section 20 of the FTC Act. 15 U.S.C. § 57b-1(e).

5. On January 3, 2008, the Commission issued a “Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security.” The resolution authorized any and all compulsory process available to the Commission to be used in investigations

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. 45, as amended.

File No. P954807 (Jan. 3, 2008).

6. In 2009, FTC staff learned that some consumers’ personally-identifiable and sensitive health information was available on easily-accessible

peer-to-peer (“P2P”) file sharing networks, Pet. Exh. 1 ¶ 4, a matter that raised concern in light of the ease with which users share and transfer files and information directly between individual computers on P2P networks. *See, e.g.*, FTC Staff Report, “Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues,” *available at* <http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf> (June 2005); *see also United States v. Gabel*, No. 10-60168, 2010 WL 3927697, at *2 & n.3 (S.D. Fla. Sep. 16, 2010)(describing the operations of P2P networks).

7. Staff undertook an inquiry to determine whether disclosures of consumers’ sensitive personal information were attributable to failures to employ reasonable data security measures in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or whether they violated any other statutes or regulations enforced by the Commission. Pet. Exh. 1 ¶ 4. As part of this inquiry, Commission staff consulted with several third parties with expertise in P2P networks, including Tiversa, Inc. *Id.*

8. In the course of this inquiry, the Commission issued a CID in order to obtain copies of electronic files that were located on P2P networks and that contained sensitive information. Pet Exh. 1 ¶ 5. Included among those files was a spreadsheet (the “1,718 File”) that contained personally-identifiable information

and sensitive health information for about 9,000 LabMD patients, including patient names, Social Security numbers, birth dates, health insurance provider names and policy numbers, and medical treatment codes. *Id.*

9. In 2010, after reviewing the files and consulting with other law enforcement agencies, FTC staff expanded the investigation by issuing voluntary access requests to several of these entities, including LabMD. Pet. Exh. 1 ¶ 6. The purpose of these access letters was to determine if these entities had violated laws enforced by the Commission by failing to use reasonable and appropriate security measures to safeguard sensitive information. *Id.*

10. Though LabMD responded to the Commission's voluntary access requests, there were gaps in the materials and information produced. Pet. Exh. 1 ¶ 7. Accordingly, on December 21, 2011, the Commission issued separate CIDs, duly signed by a member of the Commission, to LabMD and Mr. Daugherty, pursuant to Resolution P954807 quoted above. *Id.*; *see also* Pet. Exhs. 2, 3.

11. The CIDs sought to complete the investigation by obtaining information about, *inter alia*, LabMD's written and informal data security policies and practices and Mr. Daugherty's involvement in these practices. Pet. Exh. 1 ¶ 7; Pet. Exhs. 2, 3. To this end, the CIDs directed Mr. Daugherty and one or more representatives of LabMD to appear and testify at investigational hearings with

FTC staff. Pet. Exhs. 2, 3. The CIDs further required LabMD and Mr. Daugherty to respond to a limited set of interrogatories, and also required LabMD to respond to a single request for documents related to its data security practices that had not already been produced to the Commission in response to the voluntary access requests. *Id.* The CIDs instructed LabMD and Mr. Daugherty to provide the interrogatory responses and documents by January 13, 2012, and scheduled the investigational hearings for January 23, 2012. *Id.* Finally, the CIDs required the recipients to certify that they had complied with the CID requirements. *Id.*

12. Commission Rule 2.7(d)(1) provides a procedure for the recipient of a subpoena to file a petition to quash or limit the subpoena that raises “all assertions of privilege or other factual or legal objections to the . . . civil investigative demand” within twenty days of the date of service. 16 C.F.R. § 2.7(d)(1).

Commission Rule 2.7(f) further provides that a petitioner may request review of an initial ruling on a petition to quash by the full Commission. 16 C.F.R. § 2.7(f).

13. On January 10, 2012, pursuant to Commission Rule 2.7(d), 16 C.F.R. § 2.7(d), LabMD and Mr. Daugherty filed timely petitions to limit or quash the CIDs. Pet. Exhs. 4, 5. In their petitions, LabMD and Mr. Daugherty raised a number of claims challenging the FTC’s authority to investigate their data security practices. *See generally* Pet. Exh. 4.

14. By letter ruling, Commissioner Julie Brill denied the petitions to limit or quash on April 20, 2012, finding the arguments factually and legally unsupported. Pet. Exh. 6. Commissioner Brill's ruling set a deadline of May 11, 2012, for all responses other than testimony and ordered that investigational hearings be held at such dates and times as Commission staff may direct in writing. *Id.* at 13. The ruling notified LabMD and Mr. Daugherty of their right to request review of the ruling by the full Commission, but noted that such review would not stay the ruling's compliance schedule. *Id.* at 1-2.

15. On April 25, 2012, pursuant to Commission Rule 2.7(f), 16 C.F.R. § 2.7(f), LabMD and Mr. Daugherty submitted a request for review by the full Commission. Pet. Exh. 7. On June 21, 2012, the Commission affirmed the April 20, 2012, ruling denying the petitions to limit or quash the CIDs. Pet. Exh. 8.

16. On June 25, 2012, following the Commission's ruling, FTC staff contacted respondents to discuss compliance with the CIDs. Pet. Exh. 1 ¶ 11. In response, by letter dated June 29, 2012, respondents renewed the objections raised in their unsuccessful petitions to quash and refused to make any representations regarding any plans to comply with the CIDs. Pet. Exh. 9. To date, LabMD and Mr. Daugherty have taken no steps to comply. Pet. Exh. 1 ¶ 12.

17. The CIDs are within the Commission's authority; the information and

documents sought are reasonably relevant to the Commission's investigation; and the CIDs do not impose an unreasonable burden on either respondent. Further, respondents' failure to comply with the CIDs greatly impedes the Commission's ongoing investigation, and prevents the Commission from completing its investigation in a timely manner. Pet. Exh. 1 ¶ 13.

Prayer for Relief

WHEREFORE, the Commission invokes the aid of this Court and prays:

- a. For the immediate issuance of an order directing respondents to appear and show cause why they should not comply in full with the CIDs;
- b. For a prompt determination of this matter and an order requiring respondents to fully comply with the CIDs within ten (10) days of such order, or at such later date as may be established by the Commission;
- c. For such other relief as this Court deems just and proper.

Respectfully submitted,

WILLARD K. TOM
General Counsel

JOHN F. DALY
Deputy General Counsel for Litigation

LESLIE RICE MELMAN
Assistant General Counsel for Litigation

BURKE W. KAPPLER
BRADLEY D. GROSSMAN
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
Telephone: (202) 326-2043 (Kappler)
Telephone: (202) 326-2994 (Grossman)
Fax: (202) 326-2477
Email: bkappler@ftc.gov
Email: bgrossman@ftc.gov

LOCAL COUNSEL:


s/ Ryan T. Holte

RYAN T. HOLTE
Georgia Bar No. 156327
CINDY A. LIEBES
Georgia Bar No. 451976
Federal Trade Commission
Suite 1500
225 Peachtree Street, NE
Atlanta, GA 30303
Telephone: (404) 656-1360 (Holte)
Telephone: (404) 656-1359 (Liebes)
Fax: (404) 656-1379
Email: rholte@ftc.gov
Email: cliebes@ftc.gov

Dated: August 29, 2012

FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL DAUGHERTY

PETITION EXHIBIT 1

Declaration of Alain Sheer

2. I am authorized to execute a declaration verifying the facts that are set forth in the Petition of the Federal Trade Commission for an Order To Enforce Civil Investigative Demands. I have read the petition and exhibits thereto (hereinafter referred to as “Pet. Exh.”), and verify that Pet. Exhs. 2 through 9 are true and correct copies of the original documents. The facts set forth herein are based on my personal knowledge or information made known to me in the course of my official duties.
3. LabMD, Inc. is a Georgia corporation located at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia, 30339. It performs medical testing services for patients in Georgia and other parts of the United States.
4. In 2009, after learning about some consumers’ personally-identifiable information and sensitive health information available on peer-to-peer (“P2P”) file sharing networks, Commission staff began an inquiry to determine whether such disclosures were attributable to “unfair or deceptive acts or practices” in violation of Section 5 or violations of other statutes or regulations enforced by the Commission. As part of this inquiry, staff consulted with several third parties, including Tiversa, Inc., a data security and investigation firm that specialized in searching P2P networks.

5. In the course of this inquiry, using administrative compulsory process, Commission staff in the fall of 2009 obtained copies of computer files that had been found on P2P networks and contained sensitive information. The files, which apparently were related to a number of different entities, included the spreadsheet that LabMD and Mr. Daugherty now call the “1,718 File.” This spreadsheet contains personally-identifiable information and sensitive health information for about 9,000 patients, including patient names, Social Security Numbers, birth dates, health insurance provider names and policy numbers, and standardized medical treatment codes.
6. In 2010, after reviewing the files and other information and consulting with other law enforcement agencies, Commission staff formally expanded the investigation by issuing voluntary access requests (known as “access letters”) to nine of these entities, including LabMD. The purpose of these access letters was to obtain information to use to determine if these entities had violated laws enforced by the Commission (such as the Federal Trade Commission Act and the Gramm-Leach-Bliley Act) by failing to use reasonable and appropriate security measures to safeguard sensitive information. All these entities received substantially similar access letters.

LabMD provided some information and documents in response to the access letter and follow-up requests.

7. In order to fill gaps in the materials and information LabMD had produced (such as in its written and informal data security practices and Mr. Daugherty's involvement in them), staff asked the Commission to issue CIDs to LabMD and to Mr. Daugherty pursuant to resolution P954807. Resolution P954807 authorizes the use of compulsory process, including CIDs,

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.


8. The CIDs were issued on December 21, 2011. Pet. Exhs. 2 , 3. The CID to Mr. Daugherty required testimony on three topics and responses to two interrogatories; the CID to LabMD required testimony on three topics and responses to three interrogatories and also included a document request. LabMD and Mr. Daugherty did not comply and instead filed timely petitions to limit or quash the CIDs. Pet. Exhs. 4, 5.
9. On April 20, 2012, Commissioner Julie Brill, acting as the Commission's delegate, denied the petitions to limit or quash in their entirety. Pet. Exh. 6.

In response, LabMD and Mr. Daugherty requested review of Commissioner Brill's ruling by the full Commission. Pet. Exh. 7.

10. On June 21, 2012, the Commission affirmed Commissioner Brill's ruling and denied the petitions. Pet. Exh. 8.
11. On June 25, 2012, Commission staff called Stephen F. Fusco, counsel for LabMD and Mr. Daugherty, to discuss compliance with the CIDs in light of the Commission's June 21, 2012, order, and followed up with a letter as to compliance. By letter dated June 29, 2012, Mr. Fusco stated that he would not take any position about LabMD's and Mr. Daugherty's compliance with the CIDs. Pet. Exh. 9.
12. To date, Commission staff has not received any documents or information from LabMD or Mr. Daugherty in response to the CIDs or the Commission ruling denying the petitions to limit or quash.
13. LabMD's and Mr. Daugherty's failure to comply with the CIDs has burdened, delayed, and impeded the Commission's investigation.

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

Executed on 8/27, 2012.



Alain Sheer

**FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL
DAUGHERTY**

PETITION EXHIBIT 2

Civil Investigative Demand to LabMD, Inc. (Dec. 21, 2011)

(Public Version)



United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

LabMD Inc.
2030 Powers Ferry Road, Bld. 500, Suite 520 Atlanta, Ga 30339
Attn: Stephen F. Fusco, General Counsel

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

LOCATION OF HEARING
FTC - Southeast Region
225 Peachtree Street NE
Suite 1500
Atlanta, Ga. 30303

YOUR APPEARANCE WILL BE BEFORE
Alain Sheer or other duly designated person

DATE AND TIME OF HEARING OR DEPOSITION

JAN 23 2012

You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

You are required to answer the Interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

JAN 13 2012

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Ruth Yodalkin/Kevin Havens
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

5. COMMISSION COUNSEL

Alain Sheer
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

DATE ISSUED

12/21/12

COMMISSIONER'S SIGNATURE

J. Tan Ross

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about those activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

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

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature _____

Title _____

Sworn to before me this day

Notary Public

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

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

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY
AND/OR DATA SECURITY**

File No. P954807

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.


Donald S. Clark
Secretary

Issued: January 3, 2008

**CIVIL INVESTIGATIVE DEMAND SCHEDULE
FOR ORAL TESTIMONY, INTERROGATORY RESPONSE,
AND DOCUMENTS TO LABMD, INC.**

**To: LabMD, Inc.
2030 Powers Ferry Road
Building 500, Suite 520
Atlanta, Ga. 30339**

Attn: Stephen F. Fusco, General Counsel

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

- A. "And,"** as well as **"or,"** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in this Schedule all information that otherwise might be construed to be outside the scope of the specification.
- B. "Any"** shall be construed to include **"all,"** and **"all"** shall be construed to include the word **"any."**
- C. "CID"** shall mean the Civil Investigative Demand, including the attached Resolution and this Schedule, and including the Definitions, Instructions, and Specifications.
- D. "Company"** shall mean LabMD, Inc., its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
- E. "Document"** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, 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, agenda, minute, code book or label. **"Document" shall also include Electronically Stored Information.**
- F. "Each"** shall be construed to include **"every,"** and **"every"** shall be construed to include **"each."**
- G. "Electronically Stored Information" or "ESI"** shall mean 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 information created, manipulated, communicated, stored, or utilized in digital form, requiring the use of computer hardware or software. This includes, but is 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 video and sound recordings, whether stored on: cards; magnetic or electronic tapes; disks; computer hard drives, network shares or servers, or other drives; cloud-based platforms; cell phones, PDAs, computer tablets, or other mobile devices; or other storage media. "ESI" also includes such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.

H. "FTC" or "Commission" shall mean the Federal Trade Commission.

I. "Identify" shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable; and (c) documents by bates number or by title or description, date, and author.

J. "Referring to" or "relating to" shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

K. "You" and "Your" shall mean the Company.

L. The singular shall be construed to include the plural, and the plural shall be construed to include the singular.

II. INSTRUCTIONS

A. Sharing of Information: The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11 (c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. Meet and Confer: You must contact Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127, as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your response, including but not limited to a discussion of the submission of Electronically Stored Information and other electronic productions as described in these Instructions.

C. Applicable time period: Unless otherwise directed in the specifications, the applicable time period for the request shall be from January 1, 2007 until the date of full and complete compliance with this CID.

D. Claims of Privilege: If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;
2. the names, addresses, positions, and organizations of all authors and recipients of the item; and
3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

E. Document Retention: You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. See 15 U.S.C. § 50; see also 18 U.S.C. §§ 1505, 1519.

F. Petitions to Limit or Quash: Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

G. Modification of Specifications: If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

H. Procedures: This CID is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1. The taking of oral testimony pursuant to this CID will be

conducted in conformity with that section and with Part 2A of the Commission's Rules, 16 C.F.R. §§ 2.8-2.9.

I. Certification: A responsible officer or a duly authorized manager of the company shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

J. Scope of Search: This CID covers documents and information 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, and other agents and consultants, whether or not such documents and information were received from or disseminated to any person or entity.

K. Document Production: You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Ruth Yodaiken, Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Ave., NW, Mail Stop NJ-8100, Washington, DC 20001. Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS. Notice of your intended method of production shall be given by mail or telephone to Alain Sheer, at 202.326.3321, at least five days prior to the return date.

L. Document Identification: Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. 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.

M. Information Identification: Each interrogatory specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification(s) or sub-specification(s) to which it is responsive.

N. 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

CID. 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 marketing materials and advertisements shall be produced in color, and copies of other materials shall be produced in color if necessary to interpret them or render them intelligible.

O. 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 the 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);

(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;

(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 specification.

(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.
- (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.

A Bureau of Consumer Protection Production Guide is available upon request from the Commission counsel named above. This guide provides detailed directions on how to fully comply with this instruction.

P. 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 us before sending those materials to discuss whether it would be appropriate to redact the sensitive information. If that information will not be redacted, contact us to discuss encrypting any electronic copies of such material with encryption software such as SecureZip and provide the encryption key in a separate communication.

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.

Q. Certification of Records of Regularly Conducted Activity: Attached is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena the Company to testify at future proceedings in order to establish the admissibility of documents produced in response to this CID. You are asked to execute this Certification and provide it with your response.

III. SPECIFICATIONS

A. ORAL TESTIMONY

The Company is required to designate and make available one or more officers, directors, managers, employees, agents, or others that are best able and competent to testify on the following subjects:

1. The Company's information security policies, practices, training, and procedures (collectively, the "security practices").
2. Security risks, vulnerabilities, and incidents through which Company documents and information (such as information collected from or about patients) either were or could have been disclosed to unrelated third parties (collectively, "security incidents"), including, but not limited to, P2P file-sharing applications and documents such as the [REDACTED] file (also known as [REDACTED] in Civil Action File No. 2011CV207137 filed in the Superior Court of Fulton County, Georgia).
3. The roles and responsibilities of Michael J. Daugherty, individual employees, and individual contractors in (a) developing, adopting, implementing, and monitoring the security practices, and (b) responding to security incidents.

B. INTERROGATORIES

1. Identify all documents that provide a basis for your testimony pursuant to this CID.
2. Identify all documents that you reviewed or considered in preparing to testify pursuant to this CID.
3. Identify all documents relating to the Company's security practices and security incidents

that you have not already produced to the FTC.

C. DOCUMENTARY MATERIAL

- 1. Produce a copy of each document identified in the responses to Interrogatories 1, 2, and 3 that has not already been produced to the FTC.**

FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL DAUGHERTY

PETITION EXHIBIT 3

Civil Investigative Demand to Michael J. Daugherty (Dec. 21, 2011)

(Public Version)

United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Michael J. Daugherty, President
LabMD Inc.
2030 Powers Ferry Road, Bld. 500, Suite 520 Atlanta, Ga 30339

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

LOCATION OF HEARING

FTC - Southeast Region
225 Peachtree Street NE
Suite 1500
Atlanta, Ga 30303

YOUR APPEARANCE WILL BE BEFORE

Alain Sheer or other duly designated person

DATE AND TIME OF HEARING OR DEPOSITION

JAN 23 2012

You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

JAN 18 2012

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Ruth Yodanis/Kevin Havens
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

5. COMMISSION COUNSEL

Alain Sheer
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

DATE ISSUED

12/21/11

COMMISSIONER'S SIGNATURE

J. Thomas Ross

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

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



United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Michael J. Daugherty, President
LabMD Inc.
2030 Powers Ferry Road, Bld. 500, Suite 520 Atlanta, Ga 30339

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

| | |
|--|--|
| LOCATION OF HEARING FTC - Southeast Region 225 Peachtree Street NE Suite 1500 Atlanta, Ga 30303 | YOUR APPEARANCE WILL BE BEFORE Alain Sheer or other duly designated person |
| DATE AND TIME OF HEARING OR DEPOSITION JAN 23 2012 | |

You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

JAN 18 2012

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Ruth Yodaiken/Kevin Havens
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

5. COMMISSION COUNSEL

Alain Sheer
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

DATE ISSUED

12/21/11

COMMISSIONER'S SIGNATURE

J. Tom Ross

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

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

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature _____

Title _____

Sworn to before me this day

Notary Public

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

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

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY
AND/OR DATA SECURITY**

File No. P954807

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.


Donald S. Clark
Secretary

Issued: January 3, 2008

**CIVIL INVESTIGATIVE DEMAND SCHEDULE
FOR ORAL TESTIMONY AND INTERROGATORY RESPONSE
TO MICHAEL J. DAUGHERTY**

**To: Michael J. Daugherty, President
LabMD, Inc.
2030 Powers Ferry Road
Building 500, Suite 520
Atlanta, Ga. 30339**

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

A. "And," as well as "or," shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in this Schedule all information that otherwise might be construed to be outside the scope of the specification.

B. "Any" shall be construed to include "all," and "all" shall be construed to include the word "any."

C. "CID" shall mean the Civil Investigative Demand, including the attached Resolution and this Schedule, and including the Definitions, Instructions, and Specifications.

D. "Company" shall mean LabMD, Inc., its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

E. "Document" shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, 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, agenda, minute, code book or label. "Document" shall also include Electronically Stored Information.

F. "Each" shall be construed to include "every," and "every" shall be construed to include "each."

G. "Electronically Stored Information" or "ESI" shall mean 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 information created,

manipulated, communicated, stored, or utilized in digital form, requiring the use of computer hardware or software. This includes, but is 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 video and sound recordings, whether stored on: cards; magnetic or electronic tapes; disks; computer hard drives, network shares or servers, or other drives; cloud-based platforms; cell phones, PDAs, computer tablets, or other mobile devices; or other storage media. "ESI" also includes such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.

H. "FTC" or "Commission" shall mean the Federal Trade Commission.

I. "Identify" shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable; and (c) documents by bates number or by title or description, date, and author.

J. "You" and "Your" shall mean Michael J. Daugherty.

K. The singular shall be construed to include the plural, and the plural shall be construed to include the singular.

II. INSTRUCTIONS

A. **Sharing of Information:** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11 (c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. **Meet and Confer:** You must contact Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127, as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your response.

C. **Applicable time period:** Unless otherwise directed in the specifications, the applicable time period for the request shall be from January 1, 2007 until the date of full and complete compliance with this CID.

D. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;
2. the names, addresses, positions, and organizations of all authors and recipients of the item; and
3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

E. Document Retention: You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. See 15 U.S.C. § 50; see also 18 U.S.C. §§ 1505, 1519.

F. Information Identification: Each interrogatory specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification(s) or sub-specification(s) to which it is responsive.

G. Petitions to Limit or Quash: Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

H. Modification of Specifications: If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

I. Procedures: This CID is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1. The taking of oral testimony pursuant to this CID will be conducted in conformity with that section and with Part 2A of the Commission's Rules, 16 C.F.R. §§ 2.8-2.9.

J. Scope of Search: This CID covers documents and information 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, other agents and consultants, and the Company, whether or not such documents and information were received from or disseminated to any person or entity.

K. Certification: You shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

III. SPECIFICATIONS

A. ORAL TESTIMONY

Subjects for testimony will include but not be limited to the following:

1. The Company's information security policies, practices, training, and procedures (collectively, the "security practices").
2. Security risks, vulnerabilities, and incidents through which Company documents and information (such as information collected from or about patients) either were or could have been disclosed to unrelated third parties (collectively, "security incidents"), including, but not limited to, P2P file-sharing applications and documents such as the [REDACTED] file (also known as [REDACTED] in Civil Action File No. 2011CV207137 filed in the Superior Court of Fulton County, Georgia).
3. The roles and responsibilities of Michael J. Daugherty, individual employees, and individual contractors in (a) developing, adopting, implementing, and monitoring the security practices, and (b) responding to security incidents.

B. INTERROGATORIES

1. Identify all documents that provide a basis for your testimony pursuant to this CID.
2. Identify all documents that you reviewed or considered in preparing to testify pursuant to this CID.

FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL DAUGHERTY

PETITION EXHIBIT 4

**LabMD's Petition to Limit or Quash the
Civil Investigative Demand (Jan. 10, 2012)**

(Public Version)

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

IN THE MATTER OF

LabMD Inc.



**LabMD'S PETITION TO LIMIT OR
QUASH THE CIVIL INVESTIGATIVE DEMAND**

Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP

2900 K Street, NW
North Tower - Suite 200
Washington, DC 20007
Phone: (202) 625-3613
Facsimile: (202) 298-7570
Email: claudia.callaway@kattenlaw.com

Counsel for Petitioner

Table of Contents

| | <u>Page</u> |
|--|-------------|
| I. FACTUAL SUMMARY | 1 |
| A. The 1,718 File Was Illegally Downloaded By Tiversa, Inc., A Technology Corporation Using Patented Computer Technology, With The Support Of Federally-Funded Researchers At Dartmouth College | 2 |
| B. Petitioner’s Lawsuit Against Tiversa and Dartmouth College | 4 |
| II. ARGUMENT | 5 |
| A. The FTC’s Authority Under Section 45..... | 5 |
| B. There Is No Basis Under Section 45 To Support Enforcement Of The Present CID, Which Is In All Events Exceedingly Overbroad And Unduly Burdensome | 7 |
| C. The CID Should Be Quashed Because It Is Not Authorized by A Valid Resolution And Is Therefore Indefinite, Overbroad, And Incapable Of Demonstrating A Valid Exercise Of The FTC’s Section 45 Authority..... | 10 |
| D. The CID Improperly Demands Documents And Testimony Concerning Matters That Are Primarily Regulated By The Department Of Health And Human Services | 12 |
| III. CONCLUSION..... | 13 |

**LabMD'S PETITION TO QUASH
THE CIVIL INVESTIGATIVE DEMAND**

Petitioner LabMD Inc. hereby petitions the Federal Trade Commission ("FTC"), pursuant to 16 C.F.R. § 2.7(d), to quash the Civil Investigative Demand ("CID") issued to Petitioner on December 21, 2011. The FTC issued the CID pursuant to its alleged authority under Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1 and therein makes various demands, including the production of all documents related to any "security risk, vulnerability, and incidents through which [Petitioner's] documents and information [] either were or could have been disclosed to unrelated third parties."¹ Petitioner respectfully submits that the FTC lacks the authority to issue the CID in its entirety to LabMD. Accordingly, Petitioner respectfully petitions the Commission to quash the CID.²

I. FACTUAL SUMMARY

Although the present CID is worded in the broadest possible manner, it appears to be premised on the third-party download of a single document belonging to Petitioner (the "1,718 File"). The 1,718 File, which contained personally identifiable information ("PII") and protected health information ("PHI") about some of Petitioner's patients, was illegally downloaded from Petitioner's computers in February of 2008. To Petitioner's knowledge, no other incidents such as this have occurred, nor does the CID reference or allege any additional incidents (despite the absence of any limitation to the CID's testimonial and documentary requests). Therefore, and because there is no other conceivable basis for the CID, Petitioner sets forth the facts

¹ A true and correct copy of the December 21, 2011 Civil Investigative Demand is attached hereto as Exhibit A.

² This petition to quash is based on the FTC's lack of authority to issue a CID to LabMD on the basis of the 1,718 File incident. However, Petitioner explicitly reserves any and all arguments or claims concerning the CID itself in the event that the FTC is found to have the requisite authority to issue a CID targeting LabMD on the basis of the 1,718 File incident.

surrounding the 2008 download of the 1,718 File, all of which are part of the FTC's private investigation record and/or are currently being adjudicated by a federal court in a civil action that Petitioner brought against the parties who illegally downloaded the 1,718 File.

A. The 1,718 File Was Illegally Downloaded By Tiversa, Inc., A Technology Corporation Using Patented Computer Technology, With The Support Of Federally-Funded Researchers At Dartmouth College

Tiversa, Inc. is a Pennsylvania Corporation who provides peer-to-peer ("P2P") intelligence services to corporations, government agencies, and individuals based on its patented EagleVision X1 technology that can monitor over 550 million computer users daily.³ On information and belief, both Tiversa and its partner, Dartmouth College, accepted federal funds from the National Institute of Standards and Technology, the United States Department of Justice, the United States of Homeland Security, and the National Science Foundation, among other governmental agencies, to develop P2P search technology. During a 2007 congressional hearing, Tiversa testified that its proprietary technology allowed it to process 300 million searches per day, or over 170 million more searches than Google was processing per day.⁴ At the same hearing, Tiversa admitted that it had downloaded computer files containing, but by no means limited to –

federal and state identification, including passports, driver's license, 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.⁵

³ See Company Overview, Website for Tiversa, <http://www.tiversa.com/about/>.

⁴ See Tiversa's July 24, 2007 testimony before the United States House of Representatives Committee on Oversight and Government Reform, a true and correct copy of which is attached hereto as Exhibit B, at 3.

⁵ *Id.* at 5.

Two years later, in April of 2009, Dartmouth College published a paper entitled *Data Hemorrhage in the Health-Care Sector*.⁶ The paper was based upon activities “conducted in collaboration with Tiversa” using Tiversa’s proprietary technology⁷ and was financially supported by a U.S. Department of Homeland Security Grant Award issued under the auspices of the Institute for Information Infrastructure Protection.⁸ According to the paper, Tiversa and Dartmouth began their project by “looking for files from top ten publicly traded health-care firms” that were available on P2P networks.⁹ As part of the initial search, Tiversa and Dartmouth manually reviewed 3,328 computer files downloaded from P2P networks, many of which contained PII and PHI.¹⁰

Following their initial search, Tiversa and Dartmouth undertook a second search (“Second Search”) lasting approximately six months.¹¹ During the Second Search, Tiversa and Dartmouth downloaded closed to four million documents, including over 20,000 medical patient records.¹² Tiversa described the evolving technology it used for the Second Search in a 2009 hearing before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection (“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

⁶ A true and correct copy of the April 2009 paper is attached hereto as Exhibit C.

⁷ *Id.* at 1.

⁸ *Id.*

⁹ *Id.* at 8.

¹⁰ *Id.* at 9-11.

¹¹ *Id.* at 11.

¹² *Id.* at 13 (referencing the 20,000 medical patient records that were downloaded); *see also* Tiversa’s May 4, 2009 testimony before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection, a true and correct copy of which is attached hereto as Exhibit D, at 10 (referencing the nearly four million documents that were downloaded).

P2P network in its entirety in real time.”¹³ Further, Tiversa “processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day”.¹⁴ To showcase its technology, during the hearing Tiversa, performed a “live demonstration” whereby it intentionally searched for and downloaded over 275,000 tax returns.¹⁵

On July 29, 2009, Tiversa appeared before the United States House of Representatives Committee on Oversight and Government Reform and testified further about the technology it had used to perform the Second Search.¹⁶ According to its testimony, Tiversa deployed newly developed P2P search technology that allowed it to penetrate even “the most technologically advanced” computer security despite the presence of “firewalls and encryption.”¹⁷ It was with this technology, and during the Second Search, that Tiversa and Dartmouth downloaded the 1,718 File, a copy of which Tiversa produced at the 2009 CTC hearing.¹⁸

B. Petitioner’s Lawsuit Against Tiversa and Dartmouth College

Rather than agreeing to destroy its copies of the 1,718 File or explain to Petitioner how it had downloaded the 1,718 File, Tiversa solicited Petitioner on six occasions to purchase its security services in order to “remediate” any issues involving the 1,718 File.¹⁹ For example, on May 15, 2008, Tiversa informed Petitioner that any information regarding the means by which it acquired the 1,718 File “would require a professional services agreement.”²⁰ Dartmouth,

¹³ Ex. D at 3-4.

¹⁴ *Id.* at 4.

¹⁵ *Id.*

¹⁶ A true and correct copy of Tiversa’s July 29, 2009 testimony before the United States House of Representatives Committee on Oversight and Government Reform is attached hereto as Exhibit E.

¹⁷ Ex. E at 3.

¹⁸ Ex. B at 11.

¹⁹ *See infra* note 22, Ex. F at ¶¶ 72-98.

²⁰ *Id.* at ¶ 87.

meanwhile, used federal funding to publish at least two additional papers discussing the activities leading to the download of the 1,718 File.²¹

On November 23, 2011, Petitioner filed suit against Tiversa and Dartmouth alleging, among other things, computer fraud, computer crimes, conversion, and trespass.²² Tiversa, with the support of Dartmouth, was and is running an extortionist scheme whereby it uses its government-funded technology to penetrate computer networks, download confidential files, and then sell the files back to the owners under the guise of providing network security.

II. ARGUMENT

A. The FTC's Authority Under Section 45

While 15 U.S.C. § 45(a) grants the FTC the authority to investigate deceptive or unfair practices affecting commerce, this authority is not without limits. Likewise, although Congress has empowered the FTC under Section 57b-1 to issue CIDs in support of investigations undertaken pursuant to Section 45, a CID is only enforceable to the extent it rests on a legitimate exercise of Section 45 authority. In part for this reason, CIDs are not self-enforcing and the target of a CID is entitled to judicial review of a CID to prevent misuse of the FTC's statutory authority.²³

In *U.S. v. Morton Salt Co.*, the United States Supreme Court established the standard for determining when a CID should be quashed.²⁴ Although the Court enforced the decree at issue in

²¹ *Id.* at ¶¶ 100-102.

²² *LabMD Inc. v. Tiversa, Inc.*, No 1:11-cv-4044 (Nov. 30, 2011 N.D. Ga.). A true and correct copy of the Complaint is attached hereto as Exhibit F.

²³ See, e.g., *SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1024 (D.C. Cir. 1978), *cert denied*, 439 U.S. 1071 (1979) ("The federal courts stand guard, of course, against abuses of their subpoena-enforcement processes . . .") (citing *U.S. v. Powell*, 379 U.S. 48, 58 (1964) and *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186,216 (1946)); *D.R. Horton, Inc. v. Jon Leibowitz, Chairman*, No. 4:IO-CV-547-A, 2010 WL 4630210, at *2 (N.D. Tex. Nov. 3, 2010). ("As the government notes in its motion documents, the CID is not self-executing, and may only be enforced by a district court in an enforcement proceeding.").

²⁴ 338 U.S. 632 (1950).

that case, it recognized that “a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power” of the agency.²⁵ Accordingly, the Court held that agency subpoenas or CIDs should not be enforced if they demand information that is: (a) not “within the authority of the agency,” (b) “too indefinite,” or (c) not “reasonably relevant to the inquiry.”²⁶ This standard has been consistently applied by the federal judiciary.²⁷ For example, in *SEC v. Blackfoot Bituminous, Inc.*, the Court of Appeals for the Tenth Circuit confirmed that “an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”.²⁸

The costs and burdens imposed by a CID must also be considered.²⁹ An administrative agency may not use its investigative powers to go on a fishing expedition.³⁰ Rather, a CID must be based on a justifiable belief that wrongdoing has actually occurred. The Supreme Court did

²⁵ *Id.* at 652

²⁶ *Id.*

²⁷ *See, e.g., SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512 (10th Cir. 1980) (citing *Morton Salt*, 338 U.S. at 653) (confirming that “to obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”).

²⁸ *Id.* at 514; *see also Arthur Young & Co.*, 584 F.2d at 1030-31 (noting that a subpoena request must “not [be] so overbroad as to reach into areas that are irrelevant or immaterial” and that specifications must not exceed the purpose of the relevant inquiry) (internal quotation marks and citation omitted); *FTC v. Mt. Olympus Fin. LLC*, 211 F.3d 1278 (10th Cir. 2000) (“the documents requested were reasonably relevant to an inquiry clearly within the authority of the FTC”); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 471 (2d Cir. 1996) (stating that “the disclosure sought must always be reasonable”); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1993) (holding that a CID is enforceable only “if the information sought is reasonably relevant”); *FTC v. Texaco, Inc.*, 555 F.2d 862, 881 (D.C. Cir. 1977) (stating that the “the disclosure sought shall not be unreasonable”).

²⁹ *See, e.g., FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977) (a party challenging a subpoena can successfully do so on the grounds that compliance would be overly burdensome or unreasonable); *see also Phoenix Bd. Of Realtors, Inc. v. Dep't of Justice*, 521 F. Supp. 828, 832 (D. Ariz. 1981) (the government should narrow the scope of a CID when compliance may be overly burdensome).

³⁰ *See FDIC v. Garner*, 126 F.3d 1138, 1146 (9th Cir. 1997); *FTC v. Nat'l Claims Serv., Inc.*, No. S. 98-283, 1999 WL 819640, at * 1 (E.D. Cal. Feb. 9, 1999). *See also* S. Rep. 96-500 at 4, 96th Congress 1st Session (1979) (“The FTC's broad investigatory powers have been retained but modified to prevent fishing expeditions undertaken merely to satisfy its 'official curiosity.'”).

not equivocate in *FTC v. Am. Tobacco Co.* when it made clear that “[i]t is contrary to the first principles of justice to allow a search through all the respondents’ records, relevant or irrelevant, in the hope that something will turn up.”³¹ And, of course, the mere fact that a party has suffered a data security incident does not imply any wrongdoing on the part of the victimized party.³² That is especially so when (as here) there are no allegations that the petitioner violated any established public policy or that petitioner’s customers suffered any injury as a result of the data incident.³³

B. There Is No Basis Under Section 45 To Support Enforcement Of The Present CID, Which Is In All Events Exceedingly Overbroad And Unduly Burdensome

In the present case, there is no basis under Section 45 for imposing a highly burdensome CID upon Petitioner to investigate either 1) the download of the 1,718 File by Tiversa and Dartmouth specifically or, 2) Petitioner’s data security generally. As an initial matter, Tiversa and Dartmouth’s use of government-funded, highly-proprietary, and patented technology which according to Tiversa’s congressional testimony can penetrate even the most robust network security³⁴ to download the 1,718 File in February of 2008 cannot conceivably amount to an unfair or deceptive practice on the part of Petitioner. Indeed, according to Tiversa

³¹ 264 U.S. 298,306 (1924).

³² See, e.g., Holly K. Towle, Let’s Play “Name that Security Violation!”, 11 *Cyberspace Lawyer*, Apr. 2006, at 11.

³³ “Unjustified consumer injury is the primary focus of the FTC Act.” Unfairness Statement, 104 F.T.C. 949, 1073 (1984); see also *id.* at 1076 (if a public policy is not well-established, the agency will “act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury”).

³⁴ Ex. E at 3, 6, 8 (concluding that “the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies”).

itself, the security issues enabling the download of the 1,718 File were not unique to Petitioner, but were common to almost every networked computer in the country.³⁵

Likewise, the FTC cannot point to any public policy existing in February of 2008 that Petitioner violated, thereby enabling Tiversa and Dartmouth to download the 1,718 File. To date, the FTC has not enacted any rules or standards regarding issues associated with P2P networks, which is the FTC's most common remedy for problematic issues "that occur on an industry-wide basis."³⁶ And it was not until 2010 that the FTC began notifying organizations that failure to take adequate steps to protect against the security issues posed by P2P networks could result in liability under federal law.³⁷ 2010 was also the year in which the FTC first published *Peer-to-Peer File Sharing: A Guide for Business*.³⁸ Thus, by all accounts, the present CID seeks to hold Petitioner's 2008 conduct to a standard of perfect security, a standard that the FTC itself has made clear is impossible to attain.³⁹ This is not only unfair and unreasonable, but it grossly exceeds the FTC's authority under Section 45 to investigate unfair and deceptive practices as the 2008 download of the 1,718 File by Tiversa and Dartmouth is evidence of neither.

And yet, based apparently on nothing more than possession of the 1,718 File, the CID seeks, among other things, production within 30 days of all documents relating in any manner to

³⁵ *Id.*

³⁶ A Brief Overview Of The Federal Trade Commission's Investigative And Law Enforcement Authority, July 2008, Section II(b), available at <http://www.ftc.gov/ogc/brfovrw.shtm>.

³⁷ See *FTC Warns of Breach Risk From P2P File-Sharing*, 9 No. 3 Employer's Guide HIPAA Privacy Requirements Newsl. 4 (Apr. 2010).

³⁸ Available at <http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business>.

³⁹ See Statement of the Federal Trade Commission Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations, and the Census, Comm. on Government Reform (Apr. 21, 2004) at 4 ("The Commission recognized that there is no such thing as 'perfect' security and that breaches can occur even when a company has taken all reasonable precaution."), available at <http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf>. See also Deborah Platt Majoras, *The Federal Trade Commission: Learning from History as We Confront Today's Consumer Challenges*, 75 UMKC L. Rev. 115, 128 (2006) ("The laws and rules we enforce do not require that information security be perfect. Such a standard would be costly and unobtainable.").

all of Petitioner's security practices and policies (without temporal limitation). This is not only unduly burdensome, and therefore unenforceable,⁴⁰ but the overwhelming majority of documents related to Petitioner's security practices and policies, past and present, have nothing to do with the 2008 download of the 1,718 File. There is absolutely no basis for using the 1,718 File download as a springboard to conduct a costly and burdensome fishing expedition into Petitioner's security practices and procedures.⁴¹

The FTC's timing here is also troubling. The 2008 download of the 1,718 File was explicitly reviewed by at least two congressional committees (none of which recommended taking any course of action against Petitioner). And yet, in the three years since the download of the 1,718 File was publicized in the chambers of the Congress and elsewhere, the FTC took no action. It wasn't until Petitioner declined to engage Tiversa for "security services" for the sixth time and then sued Tiversa for theft and extortion that the FTC was compelled to issue the present CID. This unusual timing only serves to incentivize organizations to pay off Tiversa (as non-payment appears to coincide with the opening of an FTC investigation).

Taken together, the present CID vastly exceeds the FTC's authority under Section 45. The government funded download of the 1,718 File in 2008 by Tiversa and Dartmouth manifestly fails to provide any evidence whatsoever of any unfair or deceptive practice by Petitioner. Consequently, the 1,718 File download (and the facts surrounding the download) not only does not provide a basis for a further FTC investigation into the download itself vis-a-vis

⁴⁰ See *FTC v. Texaco, Inc.*, 555 F.2d at 882) (respondent should not have "to cull its files for data" that would "impose and undue burden" and finding that a subpoena requiring production of "all documents that in any way reference" the issue in question "would be unduly burdensome").

⁴¹ When a CID makes demands "of such a sweeping nature and so unrelated to the matter properly under inquiry" such that they are not "reasonably relevant", they should not be enforced. See *Morton Salt Co.* 228 U.S. at 652; see also *In re Sealed Case (Administrative Subpoena)*, 42 F.3d 1412, 1420 (D.C. Cir. 1994) (remanding to the district court to determine whether the information requested related to a "valid purpose" of the agency's investigation).

Petitioner, but it emphatically does not provide any basis for a deeply burdensome, open-ended investigation into all of Petitioner's past and present security practices and procedures. As a result, the present CID should be quashed.

C. The CID Should Be Quashed Because It Is Not Authorized by A Valid Resolution And Is Therefore Indefinite, Overbroad, And Incapable Of Demonstrating A Valid Exercise Of The FTC's Section 45 Authority

Under 16 C.F.R. § 2.6, "any person under investigation compelled or requested to furnish information or documentary evidence shall be advised of the purpose and scope of the investigation and of the nature of the conduct constituting the alleged violation which is under investigation and the provisions of law applicable to such violation." Courts assess the validity of a CID by looking to the purpose and scope of the investigation and the nature of the conduct constituting the alleged violation as stated in the authorizing resolution.⁴² Importantly, however, a court can look only to the resolutions (and not any outside communications) to evaluate the scope of an investigation.⁴³ Accordingly, the FTC Operating Manual provides that –

Investigational resolutions must adequately set forth the nature and scope of the investigation. The statement may be brief, but it must be specific enough to enable a court in an enforcement action to determine whether the investigation is within the authority of the Commission and the material demanded by the compulsory process is within the scope of the resolution.⁴⁴

The single resolution that purportedly supports the present CID utterly fails the FTC's own rules and operational requirements. The resolution states, in its entirety, that "the nature and scope" of the FTC's investigation is –

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.

⁴² See, e.g., *F.T.C. v. Carter*, 636 F.2d 781,789 (D.C. Cir. 1980).

⁴³ See, e.g., *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992).

⁴⁴ O.M.3.3.6.7.4.1.

Such investigation shall, in addition, determine whether the Commission action to obtain redress of injury to consumers or others would be in the public interest.

This resolution is so sweeping that it would allow the Commission to investigate any person or entity with respect to anything. Such a broad resolution is inconsistent with both 16 C.F.R. § 2.6 and the statutory resolution requirement in 15 U.S.C. § 57b-1(i).⁴⁵

In upholding a resolution that was far more specific than the resolution here, the D.C. Circuit made clear that there are limits to the FTC's use of broad, non-specific resolutions. Under the D.C. Circuit's standard, the present resolution is utterly inadequate:

The Commission equaled this standard, and allowed our examination of the relevance of their subpoena requests, by identifying the specific conduct under investigation cigarette advertising and promotion and specific statutory provisions that confer authority and duties upon the Commission. Section 8(b) of the Cigarette Labeling and Advertising Act, under which the Commission must report to Congress on the effectiveness of cigarette labeling and current practices and methods of cigarette advertising and promotion, is self-expressive of several purposes of this investigation. We can therefore say that recitation of the statutory authority itself alerts the respondents to the purposes of the investigation. ***Section 5's prohibition of unfair and deceptive practices, which, standing broadly alone would not serve very specific notice of purpose,*** is defined by its relationship to section 8(b), as is the extremely broad and non-specific statutory authority to compile information and make reports to Congress conferred upon the Commission in section 6 of the FTC Act. The Commission additionally defined the application of section 5 in the Resolution by relating it to the subject matter of the investigation "the advertising, promotion, offering for sale, sale, or distribution of cigarettes...." We thus feel comfortably apprised of the purposes of the investigation and subpoenas issued in its pursuit, and suspect that respondents, who may feel less comfortable, are also quite aware of the purposes of the investigation.⁴⁶

Here, the bare recitation of Section 5's "prohibition of unfair and deceptive practices ...

⁴⁵ The resolution also cannot be justified as a "blanket resolution." As the FTC Operating Manual states, blanket resolutions are only appropriate "in a limited number of instances", such as to authorize second requests in antitrust investigations. O.M. 3.3.6.7.4.3.

⁴⁶ *F.T.C. v. Carter*, 636 F.2d 781,788 (D.C. Cir. 1980) (emphasis added).

stands broadly alone”. Accordingly, the resolution fails to reasonably define the nature and scope of the present investigation, and is therefore both invalid and incapable of providing the necessary support for the present CID. Consequently, the present CID should be quashed.

D. The CID Improperly Demands Documents And Testimony Concerning Matters That Are Primarily Regulated By The Department Of Health And Human Services

The CID should also be quashed because it demands documents and information concerning data security information over which the United States Department of Health and Human Services (“HHS”) has exclusive administrative and enforcement authority. As a healthcare sector corporation, Petitioner was at all times relevant to the 2008 download of the 1,718 File regulated by HHS with respect to the privacy rules and patient data security requirements related to PHI under the Health Insurance Portability and Accountability Act (“HIPAA”).⁴⁷ It is undisputed that Congress gave HHS exclusive administrative and enforcement authority over data privacy and security issues.⁴⁸ As former FTC Chairman Deborah Majoras told Congress in 2005, HIPAA and its Privacy Rule are not enforced by the FTC.⁴⁹ This understanding was affirmed before Congress a year later by FTC Associate Director Joel Winston.⁵⁰ Accordingly, it is unreasonable and unduly burdensome to subject Petitioner to the broad investigative demands made in the present CID as the FTC is not the primary regulator of data privacy and security issues in the healthcare sector, and unlike HHS, the FTC does not have

⁴⁷ 45 C.F.R. § 160.300 *et seq.*

⁴⁸ See 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000).

⁴⁹ Deborah Platt Majoras, Chairman of the Federal Trade Commission, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*, a prepared statement before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs (Mar. 10, 2005).

⁵⁰ Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, Statement of Joel Winston, a prepared statement before the U.S. House of Representatives, Subcommittee on Social Security of the House Committee on Ways and Means (Mar. 30, 2006).

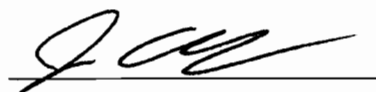
the Congressionally-delegated administrative or enforcement powers (or responsibilities) concerning these issues.

Consequently, the present CID improperly inserts the FTC into what is squarely the regulatory jurisdiction of HHS without providing any legal or policy justification for doing so. A regulated entity like Petitioner is entitled to one consistent set of data privacy and security regulations. By order of Congress, that set of regulations comes from HHS, not the FTC. Accordingly, the CID should be quashed.

III. CONCLUSION

Because the present CID was issued pursuant to an impermissible exercise of the FTC's Section 45 authority namely, because there is no basis in law or fact for using the 2008 download of the 1,718 File as grounds to conduct an unbounded, undefined, highly burdensome, and purposeless investigation into Petitioner's data security practices and policies, and further because such an investigation would impermissibly intrude upon the regulatory jurisdiction of a sister agency the present CID should be quashed.

Dated: January 10, 2012



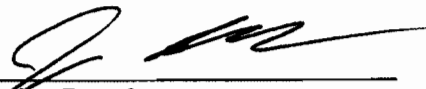
Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP
2900 K Street, NW
North Tower - Suite 200
Washington, DC 20007
Phone: (202) 625-3613
Facsimile: (202) 298-7570
Email: claudia.callaway@kattenlaw.com

Counsel for Petitioner

AMERICAN
COURT REPORTERS
ASSOCIATION

CERTIFICATION


Pursuant to 16 C.F.R. § 2.7(d)(2), counsel for Petitioner hereby certifies that counsel met and conferred with FTC counsel in a good faith effort to resolve by agreement the issues set forth in this Petition, but the parties were unable to reach agreement.



Julian Dayal

CERTIFICATE OF SERVICE

I hereby certify that on the 10th day of January, 2012, I caused the original and 12 copies of the foregoing Petition to Quash with attached exhibits to be filed by hand delivery with the Secretary of the Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, DC, 20580, and one copy of same to be filed by hand delivery with Alain Sheer, Esq., Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Avenue, N.W., Washington, D.C., 20580.



Julian Dayal



United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

LabMD Inc.
2030 Powers Ferry Road, Bld. 500, Suite 520 Atlanta, Ga 30339
Attn: Stephen F. Fusco, General Counsel

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

LOCATION OF HEARING
FTC - Southeast Region
225 Peachtree Street NE
Suite 1500
Atlanta, Ga. 30303

YOUR APPEARANCE WILL BE BEFORE
Alain Sheer or other duly designated person

DATE AND TIME OF HEARING OR DEPOSITION

JAN 23 2012

You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

You are required to answer the Interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

JAN 13 2012

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Ruth Yodanis/Kevin Havens
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

5. COMMISSION COUNSEL

Alain Sheer
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

DATE ISSUED

12/21/12

COMMISSIONER'S SIGNATURE

J. Tom Ross

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

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

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature _____

Title _____

Sworn to before me this day

Notary Public

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

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

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY
AND/OR DATA SECURITY**

File No. P954807

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.


Donald S. Clark
Secretary

Issued: January 3, 2008

**CIVIL INVESTIGATIVE DEMAND SCHEDULE
FOR ORAL TESTIMONY, INTERROGATORY RESPONSE,
AND DOCUMENTS TO LABMD, INC.**

**To: LabMD, Inc.
2030 Powers Ferry Road
Building 500, Suite 520
Atlanta, Ga. 30339**

Attn: Stephen F. Fusco, General Counsel

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

- A. “And,”** as well as **“or,”** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in this Schedule all information that otherwise might be construed to be outside the scope of the specification.
- B. “Any”** shall be construed to include **“all,”** and **“all”** shall be construed to include the word **“any.”**
- C. “CID”** shall mean the Civil Investigative Demand, including the attached Resolution and this Schedule, and including the Definitions, Instructions, and Specifications.
- D. “Company”** shall mean LabMD, Inc., its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
- E. “Document”** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, 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, agenda, minute, code book or label. **“Document” shall also include Electronically Stored Information.**
- F. “Each”** shall be construed to include **“every,”** and **“every”** shall be construed to include **“each.”**
- G. “Electronically Stored Information” or “ESI”** shall mean 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 information created, manipulated, communicated, stored, or utilized in digital form, requiring the use of computer hardware or software. This includes, but is 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 video and sound recordings, whether stored on: cards; magnetic or electronic tapes; disks; computer hard drives, network shares or servers, or other drives; cloud-based platforms; cell phones, PDAs, computer tablets, or other mobile devices; or other storage media. "ESI" also includes such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.

H. "FTC" or "Commission" shall mean the Federal Trade Commission.

I. "Identify" shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable; and (c) documents by bates number or by title or description, date, and author.

J. "Referring to" or "relating to" shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

K. "You" and "Your" shall mean the Company.

L. The singular shall be construed to include the plural, and the plural shall be construed to include the singular.

II. INSTRUCTIONS

A. Sharing of Information: The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11 (c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. Meet and Confer: You must contact Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127, as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your response, including but not limited to a discussion of the submission of Electronically Stored Information and other electronic productions as described in these Instructions.

C. Applicable time period: Unless otherwise directed in the specifications, the applicable time period for the request shall be from January 1, 2007 until the date of full and complete compliance with this CID.

D. Claims of Privilege: If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;
2. the names, addresses, positions, and organizations of all authors and recipients of the item; and
3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

E. Document Retention: You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. See 15 U.S.C. § 50; see also 18 U.S.C. §§ 1505, 1519.

F. Petitions to Limit or Quash: Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

G. Modification of Specifications: If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

H. Procedures: This CID is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1. The taking of oral testimony pursuant to this CID will be

conducted in conformity with that section and with Part 2A of the Commission's Rules, 16 C.F.R. §§ 2.8-2.9.

I. Certification: A responsible officer or a duly authorized manager of the company shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

J. Scope of Search: This CID covers documents and information 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, and other agents and consultants, whether or not such documents and information were received from or disseminated to any person or entity.

K. Document Production: You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Ruth Yodaiken, Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Ave., NW, Mail Stop NJ-8100, Washington, DC 20001. Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS. Notice of your intended method of production shall be given by mail or telephone to Alain Sheer, at 202.326.3321, at least five days prior to the return date.

L. Document Identification: Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. 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.

M. Information Identification: Each interrogatory specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification(s) or sub-specification(s) to which it is responsive.

N. 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

CID. 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 marketing materials and advertisements shall be produced in color, and copies of other materials shall be produced in color if necessary to interpret them or render them intelligible.

O. 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 the 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);

(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;

(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 specification.

(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.
- (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.

A Bureau of Consumer Protection Production Guide is available upon request from the Commission counsel named above. This guide provides detailed directions on how to fully comply with this instruction.

P. 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 us before sending those materials to discuss whether it would be appropriate to redact the sensitive information. If that information will not be redacted, contact us to discuss encrypting any electronic copies of such material with encryption software such as SecureZip and provide the encryption key in a separate communication.

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.

Q. Certification of Records of Regularly Conducted Activity: Attached is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena the Company to testify at future proceedings in order to establish the admissibility of documents produced in response to this CID. You are asked to execute this Certification and provide it with your response.

III. SPECIFICATIONS

A. ORAL TESTIMONY

The Company is required to designate and make available one or more officers, directors, managers, employees, agents, or others that are best able and competent to testify on the following subjects:

1. The Company's information security policies, practices, training, and procedures (collectively, the "security practices").
2. Security risks, vulnerabilities, and incidents through which Company documents and information (such as information collected from or about patients) either were or could have been disclosed to unrelated third parties (collectively, "security incidents"), including, but not limited to, P2P file-sharing applications and documents such as the [REDACTED] file (also known as [REDACTED] in Civil Action File No. 2011CV207137 filed in the Superior Court of Fulton County, Georgia).
3. The roles and responsibilities of Michael J. Daugherty, individual employees, and individual contractors in (a) developing, adopting, implementing, and monitoring the security practices, and (b) responding to security incidents.

B. INTERROGATORIES

1. Identify all documents that provide a basis for your testimony pursuant to this CID.
2. Identify all documents that you reviewed or considered in preparing to testify pursuant to this CID.
3. Identify all documents relating to the Company's security practices and security incidents

that you have not already produced to the FTC.

C. DOCUMENTARY MATERIAL

1. Produce a copy of each document identified in the responses to Interrogatories 1, 2, and 3 that has not already been produced to the FTC.

**Robert Boback
Chief Executive Officer
Tiversa, Inc.**

**Testimony Before the
House Committee on Oversight and Government
Reform**

July 24, 2007

Good morning Chairman Waxman, Ranking Member Davis and distinguished members of the committee.

My name is Robert Boback and I am Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides information technology and investigation services that help protect organizations, government agencies and individual consumers from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

I wish to extend our most sincere appreciation for inviting us to testify on this very important issue today. And I also want to applaud the Chairman for calling this important hearing and this committee's previous legislation and work on this topic.

While the Internet is a true boon to our society and economy, there are critical personal privacy and national security issues that need to be addressed seriously, urgently and with the immediate intent to find solutions.

These privacy and security threats are caused by the inadvertent misuse of P2P file sharing software, which Tiversa estimates has been installed on over 450 million computers worldwide. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the world wide web, it is not without inherent risks.

P2P technology provides an efficient way for people to share files with each other. Essentially, the technology uses the muscle power of the computers that it connects and allows people to share files directly with each other. When files are shared directly between two P2P users, this is called decentralized file sharing. This means the files do not go through any central computer server in the middle of the exchange.

P2P has gained both popularity and notoriety for the file sharing of entertainment content among its users. Yet, regardless of where one stands on P2P activity, it's unquestioned that P2P usage is rapidly growing and becoming generally accepted as the most efficient way to distribute large pieces of digital content to consumers.

Indeed, with the explosive increase in digital content including online video and user generated digital content, P2P file sharing is being embraced by many legitimate, well-known businesses to distribute and share television shows and full-length movies to consumers in a manner that protects the copyright and privacy of the content.

Therefore, P2P file sharing is becoming as much of a critical and integral part of the Internet's infrastructure as Web browsers are today. As a result, we must consider the privacy and security issues around it accordingly while allowing for legitimate uses of the technology.

Inadvertent file sharing happens when computer users mistakenly share more files than they intend. For example, they may only want to share their music files or a large academic report, but instead open all files on their computer's hard drive to access by other users on the P2P network. This typically occurs by a user error in either installing and/or using the software.

The result of inadvertent file sharing is hundreds of thousands of sensitive, confidential, and classified files are exposed and made available to the universe of P2P users each day.

Today, we would like to provide the committee with concrete examples that show the extent of how inadvertent P2P file sharing can negatively affect consumers, corporations, government entities and, indeed, our national security. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how users on P2P file sharing networks actively search for inadvertently shared sensitive information, and offer our thoughts on actions to address this problem.

Despite the tools that P2P networks are putting into their software to avoid the inadvertent file sharing of private or classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC has issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act, co-sponsored by Chairman Waxman, Ranking Member Davis and several members of this committee highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as Carnegie Mellon University's Computer Emergency Response Team (CERT) and

the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's *ST05-007-Risks of File-Sharing Technology - Exposure of Sensitive or Personal Information* clearly states:

“By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.”

Additionally, many of the most popular P2P tools prominently display similar warnings to their users.

Regardless, the problem persists, and our opinion is that it's getting worse. Here is why we hold this opinion.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can round-up all the previously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a portion of a P2P file sharing network, Tiversa can see the whole. It is our belief that no other system has this capability. We have the unique ability to observe activity across P2P networks, to see what inadvertent file sharing is taking place, and to see how P2P users are seeking this information, and where the information goes once it is shared.

Tiversa can monitor, on average, at least 300 million total P2P requests per day. We can investigate more fully to determine the intent of those requests. Our systems have the ability to record the searches for files made on P2P networks, as well as the ability to access the files available to users of P2P networks who issue these searches.

Users on a P2P networks must “ask” the network for a file before they can download them. For example, they may request “Frank Sinatra, I Did It My Way.” That search request is then broadcasted to all connected users for a response that says in effect - “I have that song”. At this point, the searcher can initiate a download request from their choice of users who possess that file.

Substitute the Sinatra search for “classified troop movements” and you begin to understand the problem. Or, if someone searches for “ABC Bank August Statement”, we can deem their intent was to obtain bank statements.

For example, Tiversa set its algorithms to record P2P search strings that matched the term “Credit Card” and separately the term “Medical.” Illustrated below is a limited set of English language examples taken from the millions of similar search strings that Tiversa observes each day:

Credit Card

| | |
|--------------------------------|----------------------------------|
| ▪ d&b credit card info | ▪ credit card pin numbers |
| ▪ corporate credit card log | ▪ credit card with cv2 numbers |
| ▪ credit card merch copy sr | ▪ credit card statements |
| ▪ davids credit card numbers | ▪ credit card comm sept private |
| ▪ credit card charge ctm costa | ▪ credit card authorisation july |
| ▪ credit card gateway ubc | ▪ credit card app pdf |
| ▪ 2007 batch of credit cards | ▪ athens mba credit card payment |
| ▪ cash credit card checks | ▪ cathys visa credit card go on |
| ▪ confidential credit card app | ▪ credit card with acc |
| ▪ credit card processing | ▪ credit card statements |

Medical

| | |
|--|-------------------------------|
| ▪ dear medical insurance my | ▪ child medical exam |
| ▪ letter re medical bills 10 th | ▪ billing medical august |
| ▪ denial of medical insurance | ▪ digital files medical trans |
| ▪ medical passwords | ▪ authorizationform medical |
| ▪ hospital records | ▪ caulfield general medical |
| ▪ comprehensive medical | ▪ medical coding and billing |
| ▪ medical release | ▪ medicine medical passwords |
| ▪ classified medical records | ▪ isilo medical |
| ▪ electronic medical record | ▪ doctors office medical exam |
| ▪ ltr medical maternity Portland | ▪ medical abuse records |

There are literally thousands of search strings that we can use to illustrate the millions of individual searches targeting sensitive information available on file sharing networks. One has to ask the question, “Why are P2P users searching for these files on a network typically used to share music and movies?” What are these users looking for? What will they do with the information once they find it?

We would now like to describe how consumers, businesses and government entities are victims of this problem by showing and describing actual examples of sensitive, confidential, and classified files inadvertently disclosed by these entities.

Individuals at Risk

P2P is a highly efficient way for a potential identity thief to gather an individual's private, privileged information that can then be used to commit ID theft, other forms of fraud, or put the individual's personal safety at risk. Yet, very few individuals are aware of this problem, let alone how to protect their information. There have been significant public awareness efforts aimed at educating consumers about phishing scams and other malicious activities. There has been very little effort made to protect consumers from inadvertently sharing information through P2P networks. Virus checking and firewalls, commonly highlighted as the solution, are not fully effective at solving inadvertent file sharing problem.

Examples of readily available documents Tiversa has been able to find on P2P file sharing networks include:

- Federal and State identification including passports, drivers licenses, and social security cards
- Dispute letters with banks, credit card companies, or insurance companies revealing account numbers, credit card numbers, insurance ID numbers and social security numbers
- Copies of individual credit check reports (e.g. Equifax Reports)
- Copies of individual bank and credit card statements
- Signed copies of health insurance cards
- Full copies of federal, state, and local tax returns
- Extensive electronic records of active usernames / ID's for online account access
- Wills and trust documents
- Mortgage and credit applications
- Life insurance applications
- Confidential medical history and records including psychiatric records
- Employment applications
- Family photographs and movies revealing children, addresses, and other personal information
- Student loan / aid applications and documents

Redacted examples that protect the privacy of individual document owners have been provided to the Committee.

In essence, whatever an individual stores on his/her computer electronically can be inadvertently shared. The impact of sharing these files not only hurts individual consumers directly, but also impacts the financial institutions, insurance firms, and government agencies who must incur the costs of fraud and investigations into wrong-doing. In these cases, consumers may hold these institutions responsible, when they themselves are exposing their own information. The lack of a mechanism to trace back to the source of the disclosure is often the issue in these cases. Fraud occurs, but consumers, corporations, and government organizations often do not know the root cause.

Corporate Breaches

Corporate inadvertent file sharing includes any entity that is not a governmental organization or an individual. No organization, regardless of its size or industry is immune from this problem. This ranges from the world's largest multi-national corporations across the financial services, insurance, defense, pharmaceutical, professional services and healthcare industries to small medical, accounting and law practices. Equally, no organizational function is immune to inadvertent file sharing. Tiversa has found files disclosed by and affecting human resources, finance, compliance, legal, research and development, sales, marketing, public relations, and the executive office.

With the increasing virtualization of corporate entities and the greater use of outsourcing, the concept of the *Extended Enterprise* has become critical to Tiversa's clients. This means that any entity entrusted with the corporations sensitive or confidential information can become a disclosure point on P2P file sharing networks. These entities include at home or virtual employees, contractors, suppliers, attorneys, consultants, accountants, or partners. These entities are almost always outside of the corporate perimeter and, therefore, outside of the direct control and enforcement of the corporation. How many times have you e-mailed a file home on which to work? Sent a confidential file to your lawyer or accountant? Inadvertent sharing over P2P file sharing networks is perfectly designed to exploit the *Extended Enterprise*. Our examples will show this.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings would put these corporations at risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information. In fact, many times we will see P2P users searching for specific file titles on a corporation. A recent example shows P2P users searching for a foreign exchange system design document for a major financial institution more than 40 times over a three week period. Tiversa knows this document is available since we obtained it as part of our work for a client.

The larger and better known a company and its brand, the greater the risks associated with searches for these corporations.

Tiversa has many examples of corporate information disclosures. Obviously, many are extremely sensitive and would put these corporations at significant risk if they were shared in a public domain. We are happy to share illustrative information with the committee in a secure environment if specific examples are needed.

The following, however, represents examples and situations that we have encountered illustrating the risk facing corporations today.

The first example illustrates a number of points relating to corporate disclosures clearly. Tiversa has discovered a third party attorney whose clients are the world's largest pharmaceutical manufacturers disclosing 436 sensitive and confidential files related those clients. The information covers, in part, pending litigation. One document, dated April 2007, is labeled "confidential" and "by hand" and addressed to Chairman Waxman with a carbon copy to Ranking Member Davis. It appears to address questions regarding drug trials of this pharmaceutical company. This is a case of an attorney who has exposed multiple pharmaceutical companies outside of their network – a clear example of extended enterprise risk.

A second case involves the exposure of the recent board minutes of one of the world's largest financial services organizations, and was disclosed by an executive assistant to one of the executive team members. This disclosure was originally found by a private investigator and reported to the corporation.

A third case involves the disclosure of the entire foreign exchange trading backbone for one of the world's largest multi-national financial firms. These files were among hundreds of confidential internal computer design and security files. As we stated earlier, P2P users were searching for these by name.

A fourth case illustrates how a contractor can expose a corporation. Tiversa observed P2P searches involving a contractor to one of our clients. Files exposed include the entire launch plan and expected growth targets for this diversified financial institution's entry into Europe. In addition, Tiversa observed these files in the possession of a P2P user in Nigeria. In this instance, a subcontractor to the initial contractor exposed our client's confidential information.

A fifth case again illustrates how a supplier can expose a corporation. Tiversa recovered the wide-area network and disaster recovery plan for a major banking institution exposed by the company to which the bank's entire trading network was outsourced.

Tiversa can provide literally hundreds of case examples like those illustrated above. In addition, we have found:

- Press releases in mark-up before their public release covering material, non-public information
- Patent related files before submission to the patent and trademark office
- Drug trial test records before FDA approval
- Legal documents including business contracts, non-disclosure agreements, term sheets, etc.
- Human resources related documents including employee reviews, executive recruiter post-interview write-ups, confidential termination and pending litigation documents, etc.
- Accounting related documents including audit reports, corporate tax records, payrolls, invoices, etc.

- Information systems related documents including administrative user ID / passwords to corporate systems, network diagrams, router access codes, functional specifications, disaster recovery plans

Highly select redacted examples that protect the privacy of individual document owners and any other sensitive information have been provided to the committee.

Given the media exposure that “lost laptops” and information disclosures on non-P2P networks has received, P2P inadvertent file sharing represents a significant brand, operational, legal, and regulatory risk to corporations. For example, a recent P2P sourced breach affecting 17,000 current and former Pfizer employees’ personal information illustrates the impact of the inadvertent sharing of sensitive information on P2P file sharing networks. Any one of the examples provided to the committee could result in a similar problem for its respective corporation.

Classified Government Data Exposed

Inadvertent P2P file sharing affects all levels and branches of government, law enforcement, and intelligence agencies. For our testimony today, Tiversa will focus on how inadvertent file sharing affects federal government agencies and law enforcement.

As with corporations, government inadvertent file sharing may originate with the agencies themselves, contractors to these agencies, soldiers or agents in the field. The same “extended enterprise” exposure problem facing corporations faces the government.

In addition, Tiversa regularly sees P2P searches for government related information including classified information and searches that could assist law enforcement.

In 2003, Chairman Waxman, Ranking Member Davis and many members of this committee co sponsored the Government Network Security Act. It was designed to quite simply: “require Federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by peer-to-peer file sharing.”

In a press release announcing the Act, Ranking Member Davis was quoted saying, “Few people recognize these risks. Using these programs is similar to giving a complete stranger access to your personal file cabinet.”

Unfortunately, while the bill passed the House, it stalled in the Senate. Now, four years later, there are hundreds, if not thousands, of examples of federal government classified documents publicly available on P2P networks at this very moment.

A stark example is the discovery of 34 classified documents available and found by Tiversa on P2P networks. At least one of these classified examples was

related to a government contractor. At least one of the classified documents is the secret property of the United Kingdom, which shows the inadvertent release of such sensitive data is unquestionably global in nature.

Prior to our testimony today, Tiversa provided secret classified documents we located to General Wesley Clark, an equity holding member of Tiversa's advisory board. He has since furnished these documents to the Chairman of the National Intelligence Advisory Board for investigation. This information could, and most likely does, pose significant risks to our interests domestically and abroad. Unfortunately, this is not an isolated incident.

Inadvertently shared information is not limited to classified information. A diverse amount of information exists across government agencies and contractors. Here are some examples:

1. A document illustrating over 100 individual soldier's names and social security numbers
2. Physical Threat Assessments for multiple cities such as Philadelphia, St. Louis, and Miami
3. A government contractor exposing an air force base physical security attack assessment
4. A document titled "*NSA Security Handbook*"
5. A detailed report from a well known government contractor for the National Security Agency (NSA) which outlines how to connect two secure DoD networks
6. Numerous Department of Defense Directives (DoDD's) on various Information Security topics – all signed by various Assistant and Deputy Secretaries of State
7. Various Department of Defense Information Security system audits, reviews, procedures, etc. (e.g. retina scanner equipment audits, penetration detection software/equipment reviews)
8. Numerous "Field Security Operations" documents including router checklist procedures, "Network Infrastructure Security Checklist", etc.
9. Numerous presentations for Armed Forces leadership on various Information Security topics including how to profile "hackers" and potential internal information leakers
10. Large numbers of army documents marked "For Official Use Only"

A case example illustrates the risks clearly. On July 17, 2007, Tiversa found a defense contractor employee disclosing 1,900 individual files from one IP address on P2P file sharing networks. This contractor supports 34 "Joint and Army agencies", including the Department of Defense at the Pentagon, Defense Intelligence Agency, National Security Agency, US Air Force, Army, Navy and the National Imagery and Mapping Agency. This person was disclosing a wide array of files including music, personal information, resumes, photos, etc. Alarming, this individual was also disclosing 534 files with extremely sensitive, privileged information regarding the US Government generally, and the Department of

Defense and various US Armed Forces specifically. The types of information disclosed included:

- The entire Pentagon secret backbone network infrastructure diagram including server/IP addresses
- Password change scripts for Pentagon secret network servers
- Department of Defense employees contact information (including cell and home phone numbers)
- Secure Sockets Layer (SSL) instructions and certificates allowing access to the disclosing contractors' IT systems
- A contract issued by the "Army Contracting Agency" at the Pentagon that authorizes expenditures in excess of \$1.5 million with the disclosing contractor
- Numerous policies/procedures regarding the Pentagon's IT infrastructure as well as its threat response activities (including a "Draft Strategic Plan" for 2007 – 2011)
- A letter from a "Deputy Director for Management" at the "Executive Office of the President's Office of Management and Budget" which explicitly talks about some of the risks associated with P2P file sharing networks.

Ironically, it appears that the individual disclosing this information could be a member of a computer incidence response team and could hold top secret clearance – certainly not an uninformed computer user.

The risks posed by this disclosure source are widespread. For one, the disclosed information could be used directly to penetrate the Pentagon's secure IT environment in an effort to access highly classified information. Secondly, the information could be used indirectly against the disclosure source for blackmail, coercion, kidnapping, etc.

Outside of the alarming nature of this instance, this case clearly illustrates a number of key points:

- Extended Enterprise Risks – these disclosures appear to have happened *outside* of the Pentagon's network where traditional perimeter IT approaches and policies are not effective.
- One Source / Many Exposures – one source, in this case, adversely affected multiple government agencies. This exposure is worse than a lost laptop since P2P users have open access to the information on the computer without the knowledge of the owner. Anyone who knows what to look for can obtain this information and share it.
- Risk of "Open Windows" – whatever new files are now added to this individual's computer will then become available to the P2P user community. Despite the fact that sensitive files may or may not be

present on an employee or suppliers computer today, the very existence of P2P file sharing software can expose whatever files are added in the future.

Redacted examples that protect the privacy of the respective government agencies and affected individuals have been provided to the Committee with the exception of classified information which, as noted earlier, was provided to the Chairman of the National Intelligence Advisory Board by General Wesley Clark.

Law Enforcement Related Examples

Citizens expect our government to protect its own classified and confidential information, but to also enforce laws governing illegal uses and exploitation of information. Examples of this include enforcing copyright and licensing laws and export control laws. One example we wish to highlight to the committee is the extensive use of P2P Networks for searching and sharing child pornography. To illustrate the extent of this trafficking of this information, Tiversa collected searches that P2P users were issuing for known child pornography terms. This example is provided to the committee as a separate exhibit.

Live Demonstration

While the examples collected represent various periods of time, a glimpse into what is available *live* on P2P networks dramatically illustrates the extent of exposure for the categories of examples highlighted above. We will now show user issued searches and available files that match a select list of file probing terms.

Evidence of Wrong-doing

Tiversa has shown the committee live views of P2P user issued searches and available sensitive, inadvertently shared files. We have illustrated that P2P users are actively searching for sensitive, confidential, and classified information. We have shown sensitive, confidential, and classified files are present on P2P networks across individual consumer, corporate, and government sources. What happens to these files once they are found, downloaded, replicated, or used? Is there evidence of fraud or wrong doing?

Fraud Test

Tiversa, in conjunction with Dartmouth's Center for Digital Strategies, conducted a test to show that once a file with actionable financial information is inadvertently disclosed on a P2P network, individuals will use it for an ill-gotten financial gain.

Tiversa and Dartmouth purchased a VISA cash card and an AT&T calling card and incorporated the cash card numbers and phone card numbers instructions on how to use these into a letter. An electronic copy of the letter was put on a

Dartmouth test computer and shared using LimeWire file sharing software. Tiversa tracked the spread of the letter globally across P2P file sharing networks, from the point of initial compromise from the original source computer to its sharing and subsequent re-sharing(s). Tiversa and Dartmouth then tracked the real-time use of the cash card and calling card. The VISA cash card was depleted within a week. Even after the original source computer was shut off, the file continued to be shared by others users on P2P file sharing networks.

Professor Eric Johnson from Dartmouth will explain this test in more detail in later testimony to this committee.

Corporate Information Test

A similar Dartmouth experiment was conducted with documents related to a fictitious company placed on a Dartmouth test computer and shared using LimeWire file sharing software. Tiversa then tracked the spread of these files from the original source computer across P2P networks clearly indicating that there was significant "demand" for these "corporate" files.

The Root of the Problem

Why is there such a pervasive and massive amount of sensitive, classified, and confidential information available on peer-to-peer file sharing networks? Corporations and government agencies have installed technologies designed to block access to P2P networks and instituted policies that prohibit employees from using P2P networks or taking or e-mailing information to their homes. Consumers have installed virus checking and firewalls, which is typically the recommended course of action by the world's major security software providers.

Tiversa's focus has been working with corporations, government agencies, and consumers to mitigate P2P disclosures and risks. Based on our experience, we believe the reason so much information is present is driven by these factors:

1. A lack of awareness to the pervasiveness and magnitude of sensitive and classified information present on P2P networks. One cannot "fix" a problem that one is unaware of, no matter how much it currently may affect an organization.
2. Overextended information security functions and budgets that prioritize recent "fires" or compliance with legislation and industry mandates. Prioritizing something to which there is little awareness is often not done because it is difficult to gain the attention of senior management and procure budgets and resources.
3. Organizations have "too narrow" a view of their network perimeter. Whose responsibility is it to protect information once it leaves the corporate perimeter? Does a consumer or the US government care

whether a corporation or a supplier to that corporation entrusted with sensitive information disclosed files on P2P File Sharing Networks once the damage is done? The overwhelming evidence shows that a substantial amount of P2P inadvertent file sharing breaches come from an organization's *Extended Enterprise* outside of its network perimeter. Many organizations today focus solely on protecting their network perimeters when their business is becoming more virtual and outsourcing is taking hold. Sensitive, confidential, and classified information follows these new business operations.

Finding Solutions

We would like to provide the committee our initial recommendations on how consumers, corporations, and government entities can mitigate this problem.

The committee should take steps to:

- Create broader and more focused awareness of the dangers of inadvertent P2P file sharing.
- Require continuous auditing of P2P file sharing networks themselves for sensitive, confidential, and classified information disclosures.
- Encourage organizations to adopt policies and to take steps to address their *Extended Enterprise*.

Consumers:

For consumers, Tiversa has a number of recommended actions

- Consumers first need to become aware of this problem. While government warnings already exist, we feel the private sector can play a highly effective role in addressing this issue and in creating awareness. Banks, credit card companies, and healthcare insurance organizations can lead this effort since they are most impacted by P2P originated fraud. They are trusted by their customers and have existing communication channels available. Previous efforts to address phishing serve as a useful model.
- Consumers should consider putting their highly sensitive information on a separate PC or device disconnected from the Internet.
- Consumers should continuously audit P2P networks to ensure that unwanted files are not exposed. If they find personal or sensitive information available, they should be equipped with the knowledge of what actions to immediately take.

Corporate

For corporations, Tiversa has a number of recommended actions:

- Those tasked with managing security risks inside of an organization must be aware of the pervasiveness and magnitude of inadvertent P2P file sharing, and how it affects them. These individuals need to educate senior leadership – especially those in privacy, legal, and compliance – to the risks they face.
- Corporations need to understand their disclosed information exposure by auditing, as fully as possible by a neutral third party, the type and magnitude of their information on P2P file sharing networks.
- Corporations need to continuously monitor for new exposure points on P2P networks, and to judge the effectiveness of their policies and remedial actions.
- Corporations need to identify disclosure sources across their Extended Enterprises that expose them to inadvertent file sharing risks. This includes employees operating outside of the perimeter, suppliers and contractors, agents, and partners.
- Corporations should re-evaluate “four wall” perimeter approaches to information security and update their policies to address information disclosure by third parties and the general lack of control once information exits an organization. This may include, for instance, requiring contractors, suppliers, attorneys, and accountants to indemnify the organization for peer-to-peer originated information disclosures.

Government

- The government should take the lead in creating greater awareness at corporations and throughout the public on the dangers associated with P2P file sharing.
- The government should immediately and continuously identify the full exposure and global spread of classified information to shut down these disclosure sources.
- The government should conduct a comprehensive audit of P2P file sharing network information disclosures – not just focused on the agencies themselves, but on also on contractors and non-agency sources.
- P2P information exposure risk should be emphasized in the Federal Information Security Management Act Report Card.

- The government should require their contractors to certify that they and their extended enterprises have fully addressed inadvertent file sharing disclosure risk.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, or classified information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of the technology in the future.

Thank you for the opportunity to testify here today.

Data Hemorrhages in the Health-Care Sector¹

M. Eric Johnson

Center for Digital Strategies
Tuck School of Business
Dartmouth College, Hanover NH 03755
M.Eric.Johnson@dartmouth.edu

Abstract. Confidential data hemorrhaging from health care providers pose financial risks to firms and medical risks to patients. We examine the consequences of data hemorrhages including privacy violations, medical fraud, financial identity theft, and medical identity theft. We also examine the types and sources of data hemorrhages, focusing on inadvertent disclosures. Through an analysis of leaked files, we examine data hemorrhages stemming from inadvertent disclosures on internet based file sharing networks. We characterize the security risk for a group of health care organizations using a direct analysis of leaked files. These files contained highly sensitive medical and personal information that could be maliciously exploited by criminals seeking to commit medical and financial identity theft. We also present evidence of the threat by examining user issued searches. Our analysis demonstrates both the substantial threat and vulnerability for the health care sector and the unique complexity exhibited by the US health care system.

Keywords: Health care information, identity theft, data leaks, security.

1 Introduction

Data breaches and inadvertent disclosures of customer information have plagued sectors from banking to retail. In many of these cases, lost customer information translates directly into financial losses through fraud and identity theft. The health-care sector also suffers such data hemorrhages, with multiple consequences. In some cases, the losses have translated to privacy violations and embarrassment. In other cases, criminals exploit the information to commit fraud or medical identity theft.

¹ Experiments described in this paper were conducted in collaboration with Tiversa who has developed a patent pending technology that, in real time, monitors global P2P file sharing networks. The author gratefully acknowledges the assistance of Nicholas Willey. This research 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). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

Given the highly fragmented US health-care system, data hemorrhages come from many different sources—ambulatory health-care providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back-offices of health maintenance organizations, and outsourced service providers such as billing, collection, and transcription firms.

In this paper we analyze the threats and vulnerabilities to medical data. We first explore the consequences of data hemorrhages, including a look at how criminals exploit medical data, in particular through medical identity theft. Next, we examine types and sources of data hemorrhages through a direct analysis of inadvertent disclosures of medical information on publically available, internet-based file sharing networks. We present an analysis of thousands of files we uncovered. These files were inadvertently published in popular peer-to-peer file sharing networks like Limewire and Bearshare and could be easily downloaded by anyone searching for them. Originating from health-care firms, their suppliers, and patients themselves, the files span everything from sensitive patient correspondence to business documents, spreadsheets, and PowerPoint files. We found multiple files from major health-care firms that contained private employee and patient information for literally tens of thousands of individuals, including addresses, Social Security Numbers, birth dates, and treatment billing information. Disturbingly, we also found private patient information including medical diagnoses and psychiatric evaluations. Finally, we present evidence, from user-issued searches on these networks, that individuals are working to find medical data—likely for malicious exploitation.

The extended enterprises of health-care providers often include many technically unsophisticated partners who are more likely to leak information. As compared with earlier studies we conducted in the banking sector (Johnson 2008), we find that tracking and stopping medical data hemorrhages is more complex and possibly harder to control given the fragmented nature of the US health-care system. We document the risks and call for better control of sensitive health-care information.

2 Consequences of Data Hemorrhages

Data hemorrhages from the health-care sector are diverse, from leaked business information and employee personally identifiable information (PII) to patient protected health information (PHI), which is individually identifiable health information. While some hemorrhages are related to business information, like marketing plans or financial documents, we focus on the more disturbing releases of individually identifiable information and protected health information. In these cases, the consequences range from privacy violations (including violations of both state privacy laws and federal HIPPA standards) to more serious fraud and theft (Figure 1).

On one hand, health-care data hemorrhages fuel financial identity theft. This occurs when leaked patient or employee information is used to commit traditional financial fraud. For example, using social security numbers and other identity information to apply for fraudulent loans, take-over bank accounts, or charge purchases to credit cards. On the other hand, PHI is often used by criminals to commit traditional medical fraud, which typically involves billing payers (e.g.,

Medicaid/Medicare or private health-care insurance) for treatment never rendered. The US General Accounting Office estimated that 10% of health expenditure reimbursed by Medicare is paid to fraudsters, including identity thieves and fraudulent health service providers (Bolin and Clark 2004; Lafferty 2007).

PHI can also be very valuable to criminals who are intent on committing medical identity theft. The crime of medical identity theft represents the intersection of medical fraud and identity theft (Figure 1). Like medical fraud, it involves fraudulent charges and like financial identity theft, it involves the theft of identity. It is unique in that it involves a medical identity (patient identification, insurance information, medical histories, prescriptions, test results...) that may be used to obtain medical services or prescription drugs (Ball et al. 2003). Leaked insurance information can be used to fraudulently obtain service, but unlike a credit card the spending limits are much higher—charges can quickly reach tens of thousands or even millions of dollars. And unlike financial credit, there is less monitoring and reporting. Sadly, beyond the financial losses, medical identity theft carries other personal consequences for victims as it often results in erroneous changes to medical records that are difficult and time consuming to correct. Such erroneous information could impact care quality or impede later efforts to obtain medical, life, or disability insurance.

For example, recent medical identity theft cases have involved the sale of health identities to illegal immigrants (Messmer 2008). These forms of theft are a problem impacting payers, patients, and health-care providers. Payers and providers both see financial losses from fraudulent billing. Patients are also harmed when they are billed for services they did not receive, and when erroneous information appears on their medical record.

Between 1998 and 2006, the FTC recorded complaints of over nineteen thousand cases of medical identity theft with rapid growth in the past five years. Many believe these complaints represent the tip of the growing fraud problem, with some estimates showing upwards of a quarter-million cases a year (Dixon 2006, 12-13). Currently, there is no single agency tasked with tracking, investigating, or prosecuting these crimes (Lafferty 2007) so reliable data on the extent of the problem does not exist.

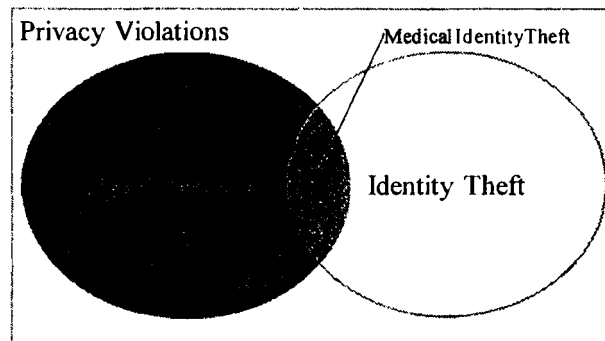


Fig. 1. Consequences of data hemorrhages.

The crime of financial identity theft is well understood with clear underlying motives. A recent FTC survey estimated that 3.7% of Americans were victims of some sort of identity theft (FTC 2007). Significant media coverage has alerted the public of the financial dangers that can arise when a thief assumes your identity. However, the dangers and associated costs of medical identity theft are less well understood and largely overlooked. Of course, PHI (including insurance policy information and government identity numbers) can be fraudulently used for financial gain at the expense of firms and individuals. However, when a medical identity is stolen and used to obtain care, it may also result in life-threatening amendments to a medical file. Any consequential inaccuracies in simple entries, such as allergy diagnoses and blood-typing results, can jeopardize patient lives. Furthermore, like financial identity theft, medical identity theft represents a growing financial burden on the private and public sectors.

Individuals from several different groups participate in the crime of medical identity theft: the uninsured, hospital employees, organized crime rings, illegal aliens, wanted criminals, and drug abusers. In many cases the theft is driven by greed, but in other case the underlying motive is simply for the uninsured to receive medical care. Without medical insurance, these individuals are unable to obtain the expensive care that they require, such as complicated surgeries or organ transplants. However, if they assume the identity of a well insured individual, hospitals will provide full-service care. For example, Carol Ann Hutchins of Pennsylvania assumed another woman's identity after finding a lost wallet (Wereschagin 2006). With the insurance identification card inside the wallet, Hutchins was able to obtain care and medication on 40 separate occasions at medical facilities across Pennsylvania and Ohio, accumulating a total bill of \$16,000. Had it not been for the victim's careful examination of her monthly billing statement, it is likely that Hutchins would have continued to fraudulently receive care undetected. Hutchins served a 3-month jail sentence for her crime, but because of privacy laws and practices, any resulting damage done to the victim's medical record was difficult and costly to erase.

Hospital employees historically comprise the largest known group of individuals involved in traditional medical fraud. They may alter patient records, use patient data to open credit card accounts, overcharge for and falsify services rendered, create phony patients, and more. The crimes committed by hospital employees are often the largest, most intricate, and the most costly.

Take for example the case of Cleveland Clinic front desk clerk coordinator, Isis Machado who sold the medical information of more than 1,100 patients, to her cousin Fernando Ferrer, Jr., the owner of Advanced Medical Claims Inc. of Florida. Fernando then provided the information to others who used the stolen identities to file an estimated \$7.1 million in fraudulent claims (USDC 2006).

Individuals abusing prescription drugs also have a motive to commit medical identity theft. Prescription drug addicts can use stolen identities to receive multiple prescriptions at different pharmacies. Drugs obtained through this method may also be resold or traded. Roger Ly, a Nevada pharmacist allegedly filed and filled 55 false prescriptions for Oxycontin and Hydrocodone in the name of customers. Medicare and insurance paid for the drugs that Ly, allegedly, then resold or used recreationally (USA 2007). The total value of drugs sold in the underground prescription market

likely exceeds \$1 billion (Peterson 2000). Sometimes, the crimes involving prescription drugs are less serious; a Philadelphia man stole a coworker's insurance identification card to acquire a Viagra prescription, which he filled on 38 separate occasions. The plan finally backfired when the coworker he was posing as attempted to fill his own Viagra prescription and discovered that one had already been filled at another pharmacy. The cost to his company's insurance plan: over \$3,000 (PA 2006).

Wanted criminals also have a strong motive to commit medical identity theft. If they check into a hospital under their own name, they might be quickly apprehended by law enforcement. Therefore, career criminals need to design schemes to obtain care. Joe Henslik, a wanted bank robber working as an ad salesman, found it easy to obtain Joe Ryan's Social Security number as part of a routine business transaction (BW 2007). Henslik then went on to receive \$41,888 worth of medical care and surgery under Ryan's name. It took Ryan two years to discover that he had been a victim of medical identity theft. Even after discovery, he found it difficult to gain access to his medical records, since his own signature didn't match that of Henslik's forgery.

Anndorie Sachs experienced a similar situation when her medical identity was used to give birth to a drug addicted baby (Reavy 2006). Sachs had lost her purse prior to the incident and had accordingly cancelled her stolen credit cards, but was unaware of the risk of medical ID theft. The baby, which was abandoned at the hospital by the mother, tested positive for illegal drug use, prompting child services to contact Sachs, who had four children of her own. Fortunately, since Sachs did not match the description of the woman who gave birth at the hospital, the problem did not escalate further. If Sachs was not able to prove her identity, she could have lost custody of her children, and been charged with child abuse. Furthermore, before the hospital became aware of the crime, the baby was issued a Social Security number in Sachs name, which could cause complications for the child later in life. Like Sachs, few individuals consider their insurance cards to be as valuable as the other items they carry in their wallet. Moreover, medical transactions appearing on a bill may not be scrutinized as closely as financial transactions with a bank or credit card.

Illegal immigrants also represent a block of individuals with a clear motive to commit medical identity theft. In the case of a severe medical emergency, they will not be refused care in most instances, but if an illegal immigrant requires expensive surgery, costly prescriptions, or other non-emergency care, they have few options. One of the most shocking and well documented cases comes from Southern California, where a Mexican resident fooled the state insurance program, Medi-Cal, into believing that he was a resident and therefore entitled to health care coverage (Hanson 1994). Mr. Hermillo Meave, was transferred to California from a Tijuana, Mexico hospital with heart problems, but told the California hospital that he was from San Diego, and provided the hospital with a Medi-Cal ID card and number. Although the circumstances surrounding Mr. Meave's arrival were suspicious, the hospital went ahead and completed a heart transplant on Mr. Meave. The total cost of the operation was an astounding one million dollars. Only after the surgery did the hospital determine that Mr. Meave actually lived and worked in Tijuana and was therefore not entitled to Medi-Cal coverage.

Perhaps emboldened by the success of Hermillo Meave, a family from Mexico sought a heart transplant for a dying relative just three months later at the very same

hospital. This time, fraud investigators were able to discover the plot before the surgery could be completed. While processing the paperwork for the patient who was checked in as Rene Garcia, Medi-Cal authorities found nine other individuals around the state, using the same name and ID number. The hospital had the family arrested and jailed for the attempted fraud, which had cost the hospital \$200,000, despite the lack of surgery. The family told investigators that they had paid \$75,000 in order to obtain the ID and set up the surgery. The trafficking of identities between Mexico and California is commonplace, but the sale of Medi-Cal identities adds a new dimension to the crime. The disparity in care between California hospitals and Mexican facilities makes the motivation to commit medical identity theft clear: falsified identification is a low-cost ticket to world-class care.

Finally, identity theft criminals often operate in crime rings, sometimes using elaborate ruses to gather the identities of hundreds of individuals. In a Houston case, criminals allegedly staged parties in needy areas offering medical deals as well as food and entertainment (USDJ 2007). At the parties, Medicaid numbers of residents were obtained and then used to bill Medicaid for alcohol and substance abuse counseling. The scheme even included fraudulent reports, written by 'certified' counselors. The fraudulent company managed to bill Medicaid for \$3.5M worth of services, of which they received \$1.8M. In this case, no medical care was actually administered and the medical identity theft was committed purely for financial reasons.

In summary, there are many reasons why individuals engage in medical identity theft, including avoiding law enforcement, obtaining care that they have no way of affording, or simply making themselves rich. Many tactics are used including first hand by physical theft, insiders, and harvesting leaked data. As we saw, PHI can be sold and resold before theft occurs—as in the case of the nine Garcias. The thief may be someone an individual knows well or it could be someone who they've never met.

For health-care providers, the first step in reducing such crime is better protection of PHI by: 1) controlling access within the enterprise to PHI; 2) securing networks and computers from direct intruders; 3) monitoring networks (internal and external) for PII and PHI transmissions and disclosures; 4) avoiding inadvertent disclosures of information. Often loose access and inadvertent disclosures are linked. When access policies allow many individuals to view, move, and store data in portable documents and spreadsheets, the risk of inadvertent disclosure increases.

3 Inadvertent Data Hemorrhages

Despite the much trumpeted enactment of the Health Insurance Portability and Accountability Act (HIPAA), data losses in the health-care sector continue at a dizzying pace. While the original legislation dates back to 1996, the privacy rules regulating the use and disclosure of medical records did not become effective until 2004. Moreover, the related security rules, which mandate computer and building safeguards to secure records, became effective in 2005. While firms and organizations have invested to protect their systems against direct intrusions and hackers, many recent data hemorrhages have come from inadvertent sources. For

example, laptops at diverse health organizations including Kaiser Permanente (Bosworth 2006), Memorial Hospital (South Bend IN) (Tokars 2008), the U.S. Department of Veterans Administration (Levitz and Hechinger 2006), and National Institutes of Health (Nakashima and Weiss 2008) were lost or stolen—in each case inadvertently disclosing personal and business information.

Organizations have mistakenly posted on the web many different types of sensitive information, from legal to medical to financial. For example, Wuesthoff Medical Center in Florida inadvertently posted names, Social Security numbers and personal medical information of more than 500 patients (WFTV 2008). Insurance and health-care information of 71,000 Georgia residents was accidentally posted on Internet for several days by Tampa-based WellCare Health Plans (Hendrick 2008).

The University of Pittsburgh Medical Center inadvertently posted patient information of nearly 80 individuals including names and medical images. In one case, a patient's radiology image was posted along with his Social Security number, insurance information, medications, and with information on previous medical screenings and procedures (Twedt, 2007). Harvard University and its pharmacy partner, PharmaCare (now part of CVS Caremark), experienced a similar embarrassment when students showed they could easily gain access to lists of prescription drugs bought by Harvard students (Russell 2005). Even technology firms like Google and AOL have suffered the embarrassment of inadvertent web posting of sensitive information (Clabum 2007, Olson 2006)—in their cases, customer information. Still other firms have seen their internal information and intellectual property appear on music file-sharing networks (DeAvila 2007), blogs, YouTube, and MySpace (Totty 2007). In each case, the result was the same: sensitive information inadvertently leaked creating embarrassment, vulnerabilities, and financial losses for the firm, its investors, and customers. In a recent data loss, Pfizer faces a class action suit from angry employees who had their personal information inadvertently disclosed on a popular music network (Vijayan 2007). In this paper we examine health-care leaks from a common, but widely misunderstood source of inadvertent disclosure: peer-to-peer file-sharing networks.

In our past research, we showed that peer-to-peer (P2P) file-sharing networks represented a significant security risk to firms operating within the banking sector (Johnson and Dynes, 2007; Johnson 2008). File sharing became popular during the late 1990s with rise of Napster. In just two years before its court-ordered closure in 2001, Napster enabled tens of millions of users to share MP3-formatted song files. Through its demise, it opened the door for many new P2P file-sharing networks such as Gnutella, FastTrack, e-donkey, and Bittorrent, with related software clients such as Limewire, KaZaA, Morpheus, eMule, and BearShare. Today P2P traffic levels are still growing with as many as ten million simultaneous users (Mennecke 2006). P2P clients allow users to place shared files in a particular folder that is open for other users to search. However, there are many ways that other confidential files become exposed to the network (see Johnson et al. 2008 for a detailed discussion). For example a user: 1) accidentally shares folders containing the information—in some cases confusing client interface designs can facilitate such accidents (Good and Krekelberg (2003)); 2) stores music and other data in the same folder that is shared—this can happen by mistake or because of poor file organization; 3) downloads

malware that, when executed, exposes files; or 4) installs sharing client software that has bugs, resulting in unintentional sharing of file directories.

While these networks are most popularly used to trade copyrighted material, such as music and video, any material can be exposed and searched for including databases, spreadsheets, Microsoft Word documents, and other common corporate file formats. The original exposure of this material over P2P networks is most likely done by accident rather than maliciously, but the impact of a single exposure can quickly balloon. After a sensitive file has been exposed, it can be copied many times by virtually anonymous P2P users, as they copy the file from one another and expose the file to more peers. Criminals are known to engage in the sale and trafficking of valuable information and data. In earlier studies using “honeypot” experiments (experiments that expose data for the purpose of observing how it is stolen), we showed how criminals steal and use both consumer data and corporate information (Johnson et al. 2008). When this leaked information happens to be private customer information, organizations are faced with costly and painful consequences resulting from fraud, customer notification, and consumer backlash.

Ironically, individuals who experience identity theft often never realize how their data was stolen. While there are many ways personal health-care data can be exposed, we will show in the next section how data hemorrhages in P2P networks represent a missing link in the “causality chain.” Far worse than losing a laptop or a storage device with patient data (Robenstein 2008), inadvertent disclosures on P2P networks allow many criminals access to the information, each with different levels of sophistication and ability to exploit the information. And unlike an inadvertent web posting, the disclosures are far less likely to be noticed and corrected (since few organizations monitor P2P and the networks are constantly changing making a file intermittently available to a subset of users). Clearly, such hemorrhages violate the privacy and security rules of HIPAA, which call for health-care organizations to ensure implementation of administrative safeguards (in the form of technical safeguards and policies, personnel and physical safeguards) to monitor and control intra and inter-organizational information access.

4 Research Method and Analysis

To explore the vulnerability and threat of medical information leakage, we examined health-care data disclosures and search activity in peer-to-peer file sharing networks. To collect a sample of leaked data, we initially focused on Fortune Magazine’s list of the top ten publically traded health-care firms (Fortune Magazine (Useem 2007)). Together those firms represented nearly \$70B in US health-care spending (Figure 2).

To gather relevant files, we developed a digital footprint for each health-care institution. A digital footprint represents key terms that are related to the firm—for example names of the affiliated hospitals, clinics, key brands, etc. Searching the internet with Google or P2P networks using those terms will often find files related to those institutions. With the help of Tiversa Inc., we searched P2P networks using our digital signature over a 2-week period (in January, 2008) and randomly gathered a sample of shared files related to health care and these institutions. Tiversa’s servers

and software allowed us 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). Files containing any one or combination of these terms in our digital footprint were captured. We focused on files from the Microsoft Office Suite (Word, Powerpoint, Excel, and Access). Of course, increasing the number of terms included in the digital footprint increases the number file matches found, but also increases false positives—files captured that have nothing to do with the institution in question. Given the large number of hospitals within these ten organizations (more than 500), our goal was to gather a sample of files to characterize the ongoing data hemorrhage. Since users randomly join P2P networks to get and share media (and then depart), the network is constantly changing. By randomly sampling over a 14-day period, we collected 3,328 files for further (manual) analysis.

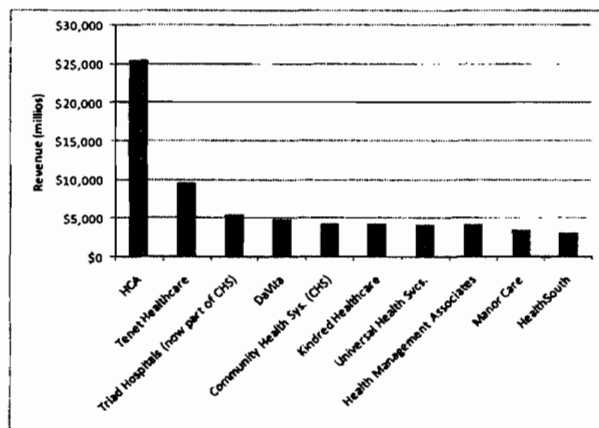


Fig. 2. Revenue of the top ten US health-care firms (Useem 2007).

Of 3,328 documents in our sample, 50.3% could be immediately identified as duplicate copies of the same file (same hash) that had spread or were on multiple IP addresses, leaving us with 1,654 documents to categorize. While duplicate files were not downloaded from the same IP address, duplicate files were collected when a target file had spread to multiple sharing clients. They were also collected from users who joined the network at different IP addresses (what we call an IP shift). Through a manual analysis of the remaining 1,654 files, we found that 71% were not relevant to health care or the organizations under consideration and were downloaded because our search terms overlapped with other subject matter. This was the result of the size and quality of our digital footprint. By casting a large net, we found more files but also many that were not related to the health-care sector. Of the remaining 475 documents, 86 were manually evaluated as duplicate files. With this cross section of

data associated with the health-care organizations, we categorized each file evaluating the dangers associated with it. Figure 3 shows a categorization of the 389 unique, relevant files.

The most common type of files found were newspaper and journal articles, followed by documents associated with students studying medicine. This should not come as a surprise as many P2P users are students. Interestingly, we found entire medical texts being shared. We also found many documents dealing directly with medical issues, such as billings, letters to hospitals, and insurance claims. Many of these documents were leaked by patients themselves. For example, we found several patient-generated spreadsheets containing details of medical treatments and costs—likely for tax purposes. Other documents discovered included hospital brochures and flyers, which were intended for public consumption. Finally there were job listings, cover letters, and résumés, all likely saved on computers of job-seekers. The lack interest in sharing these files for a typical P2P user makes it readily apparent that they were likely shared by mistake. However, all of the files weren't so innocuous. After categorizing the files, we found that about 5% of the files recovered by our loosely tuned search were sensitive or could be used to commit medical or financial identity theft.

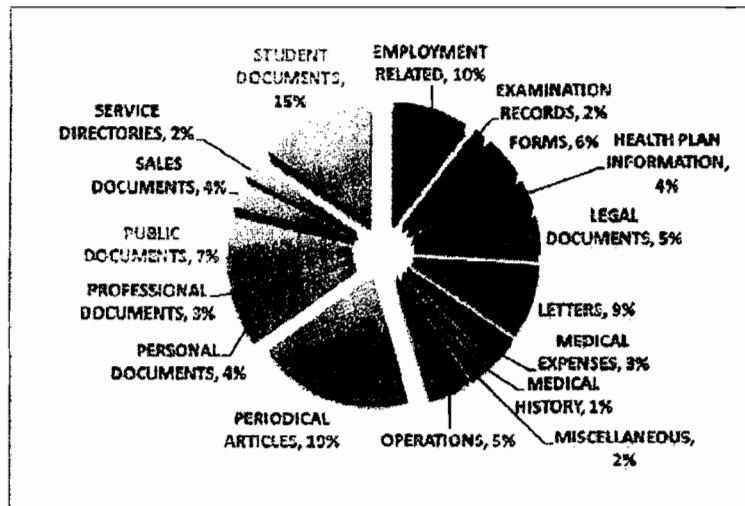


Fig. 3. Summary of unique relevant files.

The set of dangerous documents discovered contained several files that would facilitate medical identity theft. One such document was a government application for employment asking for detailed background information. The document contained the individual's Social Security number, full name, date of birth, place of

birth, mother's maiden name, history of residence and acquaintances, schooling history, and employment history (the individual had worked at one of the hospitals under study). Despite the document's three-page forward highlighting the privacy act measures undertaken by the government to protect the information in the document, and the secure Data Hash code stamped at the bottom of every page along with the bolded text 'PRIVACY ACT INFORMATION', this document somehow ended up on to a P2P network.

More disturbing, we found a hospital-generated spreadsheet of personally identifiable information on recently-hired employees including Social Security numbers, contact information, job category etc. Another particularly sensitive document was an Acrobat form used for creating patient prescriptions. The scanned blank document was signed by a physician and allowed for anyone to fill in the patient's name and prescription information. This document could be used for medical fraud by prescription drug dealers and abusers. Additionally, the doctor's own personal information was included in the document, giving criminals the opportunity to forge other documents in his name. Finally, another example we found was a young individual's medical card. This person was suffering from various ailments and was required to keep a card detailing his prescription information. The card included his doctor's name, parent's names, address, and other personal information. A person with a copy of this identification card could potentially pose as the patient and attempt to procure prescription drugs. All of these dangerous files were found with a relatively simple sample of files published for anyone to find.

As a second stage of our analysis, we then moved from sampling with a large net to more specific and intentional searches. Using information from the first sampling, we examined shared files on hosts where we had found other dangerous data. One of the features enabled by Limewire and other sharing clients is the ability to examine all the shared files of a particular user (sometimes called "browse host"). Over the next six months, we periodically examined hosts that appeared promising for shared files.

Using this approach, we uncovered far more disturbing files. For a medical testing laboratory, we found a 1,718-page document containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients. Figure 4 shows a redacted excerpt of just a single page of the insurance aging report containing patient name, Social Security number, date of birth, insurer, group number, and identification number. All together, almost 9,000 patient identities were exposed in a single file, easily downloaded from a P2P network.

Insurance Aging

[REDACTED] INCORPORATED

[REDACTED]

Date of Birth: [REDACTED] Insured: Self

| Insurance: Primary ID: | Date of Birth: | Insured: | Self | | | | | | |
|-------------------------|----------------|---------------|-------------|-------------|-------------|---------------|---------------|---------------|---------------|
| [REDACTED] | 05/01/2006 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | 12/17/2006 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | 04/03/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | 28.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 28.00 | 28.00 |
| Insurance Total: | | 273.34 | 0.00 | 0.00 | 0.00 | 147.78 | 133.56 | 373.16 | 373.16 |

Date of Birth: [REDACTED] Insured: Self

| Insurance: Primary Group Number: | ID: | Date of Birth: | Insured: | Self | | | | | |
|----------------------------------|------------|----------------|--------------|-------------|-------------|-------------|-------------|--------------|--------------|
| [REDACTED] | [REDACTED] | 02/08/2006 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| [REDACTED] | [REDACTED] | 08/10/2006 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | [REDACTED] | 12/08/2008 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| Insurance Total: | | | 62.00 | 0.00 | 0.00 | 0.00 | 0.00 | 62.00 | 62.00 |

Date of Birth: [REDACTED] Insured: Self

| Insurance: Primary Group Number: | ID: | Date of Birth: | Insured: | Self | | | | | |
|----------------------------------|------------|----------------|--------------|-------------|-------------|-------------|-------------|--------------|--------------|
| [REDACTED] | [REDACTED] | 05/19/2006 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| [REDACTED] | [REDACTED] | 06/09/2006 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| Patient Total: | | | 82.00 | 0.00 | 0.00 | 0.00 | 0.00 | 82.00 | 82.00 |
| Insurance Total: | | | 62.00 | 0.00 | 0.00 | 0.00 | 0.00 | 62.00 | 62.00 |

Date of Birth: [REDACTED] Insured: Self

| Insurance: Secondary ID: | Date of Birth: | Insured: | Self | | | | | | |
|--------------------------|----------------|------------|---------------|-------------|---------------|---------------|-------------|-------------|---------------|
| [REDACTED] | 03/02/2007 | 05/04/2007 | 110.00 | 0.00 | 0.00 | 110.00 | 0.00 | 0.00 | 110.00 |
| [REDACTED] | 04/06/2007 | | -18.00 | 0.00 | 0.00 | -18.00 | 0.00 | 0.00 | -18.00 |
| [REDACTED] | 05/02/2007 | | 110.00 | 0.00 | 0.00 | 110.00 | 0.00 | 0.00 | 110.00 |
| [REDACTED] | 06/11/2007 | | 3306.00 | 0.00 | 3306.00 | 0.00 | 0.00 | 0.00 | 3306.00 |
| [REDACTED] | 03/17/2007 | | -2138.40 | 0.00 | -2138.40 | 0.00 | 0.00 | 0.00 | -2138.40 |
| [REDACTED] | 05/17/2007 | | -824.00 | 0.00 | -824.00 | 0.00 | 0.00 | 0.00 | -824.00 |
| Patient Total: | | | 450.60 | 0.00 | 217.60 | 382.00 | 0.00 | 0.00 | 450.60 |

Date of Birth: [REDACTED] Insured: Self

| Insurance: Primary ID: | Date of Birth: | Insured: | Self | | | | | | |
|------------------------|----------------|------------|--------------|-------------|-------------|-------------|-------------|--------------|--------------|
| [REDACTED] | 01/23/2007 | 03/02/2007 | 25.70 | 0.00 | 0.00 | 0.00 | 0.00 | 25.70 | 25.70 |
| [REDACTED] | | 02/23/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | | 04/24/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | | 25.70 | 0.00 | 0.00 | 0.00 | 0.00 | 25.70 | 25.70 |

Printed [REDACTED] Time [REDACTED] Page 2 of 1718

Fig. 4. Excerpt of an insurance aging report. It contains 1718 pages of patient names, social security numbers, and dates of birth, insurers, group numbers, and identification numbers (exposing nearly 9000 patients). Personally Identifiable Information has been redacted to protect the identities of the disclosers and patients.

For a hospital system, we found two spreadsheet databases that contained detailed information on over 20,000 patients including Social Security numbers, contact details, and insurance information. Up to 82 fields of information (see Figure 5) were recorded for each patient—representing the contents of the popular HCFA form. In this case, the hemorrhage came from an outsourced collection agency working for the hospital. However, besides the patients and hospital system, many other

| | | |
|---------------------------------|-----------------------------------|---------------------------------|
| 1. FAFA billNumber | 28. dischargeDate | 55. firstInsuranceName |
| 2. providerName | 29. patientMedRecNo | 56. firstInsuranceAddressLine1 |
| 3. providerAddressLine1 | 30. patientMaritalStatus | 57. firstInsuranceCity |
| 4. providerCityStateZip | 31. guarantorFirstName | 58. firstInsuranceState |
| 5. providerPhoneNumber | 32. guarantorLastName | 59. firstInsuranceZipCode |
| 6. providerFederalTaxId | 33. guarantorSSN | 60. firstPolicyNumber |
| 7. patientFirstName | 34. guarantorPhone | 61. firstAuthorizationNumber |
| 8. patientMiddleInitial | 35. guarantorAddressLine1 | 62. firstGroupName |
| 9. patientLastName | 36. guarantorAddressLine2 | 63. firstGroupNumber |
| 10. patientSSN | 37. guarantorCity | 64. firstInsuredRelationship |
| 11. patientPhone | 38. guarantorState | 65. firstDateEligible |
| 12. patientAddressLine1 | 39. guarantorZipCode | 66. firstDateThru |
| 13. patientAddressLine2 | 40. guarantorBirthDate | 67. secondInsuranceName |
| 14. patientCity | 41. guarantorEmployerName | 68. secondInsuranceAddressLine1 |
| 15. patientState | 42. guarantorEmployerAddressLine1 | 69. secondInsuranceCity |
| 16. patientZipCode | 43. guarantorEmployerAddressLine2 | 70. secondInsuranceState |
| 17. patientSex | 44. guarantorEmployerCity | 71. secondInsuranceZipCode |
| 18. patientBirthDate | 45. guarantorEmployerState | 72. secondPolicyNumber |
| 19. patientEmployerName | 46. guarantorEmployerZipCode | 73. secondGroupName |
| 20. patientEmployerAddressLine1 | 47. guarantorEmployerPhone | 74. secondGroupNumber |
| 21. patientEmployerAddressLine2 | 48. guarantorRelationship | 75. secondInsuredRelationship |
| 22. patientEmployerCity | 49. totalCharges | 76. secondDateEligible |
| 23. patientEmployerState | 50. amountBalance | 77. secondDateThru |
| 24. patientEmployerZipCode | 51. totalPayments | 78. primaryDiagnosisCode |
| 25. patientEmployerPhone | 52. totalAdjustments | 79. attendingPhysician |
| 26. caseType | 53. accidentCode | 80. attendingPhysicianUPIN |
| 27. admissionDate | 54. accidentDate | 81. lastPaymentDate |
| | | 82. providerShortName |

Fig. 5. File contents for over 20,000 patients in on inadvertent disclosure.

organizations were comprised. The data disclosed in this file well-illustrates the complexity of US health care with many different constituencies represented, including 4 major hospitals, 335 different insurance carriers acting on behalf of 4,029 patient employers, and 266 different treating doctors (Figure 6). Each of these constituents was exposed in this disclosure. Of course, the exposure of sensitive patient health-information may be the most alarming to citizens. Figure 7 shows one very small section of the spreadsheet (just three columns of 82) for a few patients (of the nearly 20,000). Note that the diagnosis code (IDC code) is included for each patient. For example, code 34 is streptococcal sore throat; 42 is AIDS; 151.9 is malignant neoplasm of stomach (cancer); 29 is alcohol-induced mental disorders; and 340 is multiple sclerosis. In total the file contained records on 201 patients with different forms of mental illness, 326 with cancers, 4 with AIDS, and thousands with other serious and less serious diagnoses.

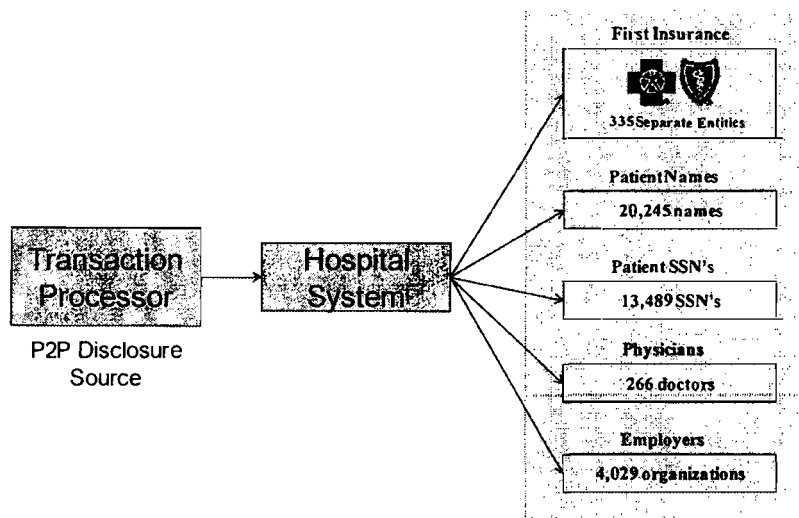


Fig. 6. Hemorrhage exposed a large array of health care constituents.

| CA | CB | CC |
|----------------------|--------------------|------------------------|
| primaryDiagnosisCode | attendingPhysician | attendingPhysicianUPIN |
| 8.45 | | |
| 34 | | |
| 34 | | |
| 34 | | |
| 42 | | |
| 151.9 | | |
| 152.1 | | |
| 291 | | |
| 291.01 | | |
| 292 | | |
| 292.02 | | |
| 340 | | |
| 340 | | |
| 780.39 | | |
| 780.39 | | |
| 780.4 | | |
| 780.6 | | |
| 780.6 | | |
| 780.79 | | |
| 780.79 | | |
| 780.99 | | |
| 789 | | |
| 798 | | |
| 923 | | |
| V70.0 | | |
| V76.12 | | |
| V76.24 | | |

Fig. 7. Disclosures expose extremely personal diagnosis information. A very small section of a spreadsheet for a few (of over 20,000) patients showing IDC diagnosis codes (see <http://www.cms.hhs.gov/ICD9ProviderDiagnosticCodes/> or <http://www.icd9data.com/>). Personally Identifiable Information has not been included in the illustration to protect the identities of the patients and physicians.

For a mental health center, we found patient psychiatric evaluations. All would be considered extremely personal and some were disturbing. We found similar clinical evaluations leaking from Alabama to Nebraska to California.

Of course, these are just few of many files we uncovered. For a group of anesthesiologists, we found over 350MB of data comprising patient billing reports. For a drug and alcohol rehab center, we found similar billing information. From an AIDs clinic we found a spreadsheet with 232 clients including address, Social Security number, and date of birth. And the list goes on. It is important to note that all of these files were found without extraordinary effort and certainly far less effort than criminals might be economically incented to undertake.

With the vulnerability well established, we also investigated the search activity in P2P networks to see if users were looking for health-care data hemorrhages. Again, using our simple digital signature we captured a sample of user-issued searches along with our files. Figure 8 lists a sample of these searches and clearly shows that users are searching for very specific health-care related data in P2P networks.

| | | | |
|--------------------------------|---------------------------------|-------------------------------|---------------------------------|
| care office nbc health | · billy connolly medical | dear medical assurance my | · letter for medical bills |
| medicine mental health crc of | · checkup | dear medical insurance my | · letter for medical bills dr |
| hospital records | · bily connoly medical check | dear medical my assurance | · letter for medical bills etmc |
| mental hospitals | · canada medical test | denial of medical insurance | · letterre medical bills 10th |
| hospital | · canadian medical | dental medical cross coding | · ltrclient medical report |
| hospital letterhead | · canadian medical association | detective medical | · ltrhjh rosimah medical |
| hospital records | · canadian medical law | digital files medical trans | · ltrmedical body4life |
| niagara hospital | · caufield general medical | distributeur medical | · ltrmedical maternity portland |
| american medical | · cbt6c1tc1 medical expenses | doctor - medical checkup | · ltrmedical misc portland |
| connolly medical ups prostate | · certificat medical | doctor fake medical by exam | · ltrorange medical head center |
| data entry medical billing fax | · certificat medical | doctor medical exam | · ltrto valley medical |
| dear medical insurance my | · certifica medical | Doctors medical billing | · lytec medical billing |
| denial of medical insurance | · certificat medical | doctors office medical exam | · medical investigation |
| hendee w r medical imaging | · charlee medical costs | doctors order medical doctor | · medical journals password |
| isilo medical | · charlee medical costs on the | doctors orders medical | · medical.txt |
| medical | · child medical exam | doug medical bill | · medical abuse records |
| medical claims | · child medical exams | doug stanhope medical pms | · medical abuse |
| medical exam | · child medical release form | edimis medical software 3.9 | · medical abuse records |
| medical history | · cigna medical dr | electronic medical | · medical algorithms |
| medical passwords | · cigna medical drs | electronic medical record | · medical authorization |
| medical permission | · classified medical records | electronic medical record osx | · medical authorization form |
| medical records certification | · complete medical exam | electronic medical record.pdf | · medical authorization |
| medical release | · comprehensive medical | electronic medical records | · medical benefits |
| medical secretary cover letter | · compudoc medical | electronic medical systems | · medical benefits plan chat |
| medicine medical passwords | · computerize medical | electronics & bio medical | · medical billing |
| authorization for medical | · computenze medical billing | emt medical software | · medical billing |
| authorization for medical of c | · tu | forms medical | · medical bill |
| authorization for medical of j | · computers in the medical offi | forms medical liability form | · medical biller resume |
| authorization form medical | · computers medical doctors | forms medical office | · medical bliig software |
| basic medical forms | · connelly medical check bily | ge medical | · medical billing |
| basic medical laboratory techn | · connelly medical ups | ge medical systems | · medical billing windows |
| benny medical jack insurance | · billing medical august | medical coding and billing | |
| billing medical | | medical coding exam | |

Fig. 8. Selection of User Issued searches that contain the word medical or hospital

5 Conclusion

Data hemorrhages from the health-care sector are clearly a significant threat to providers, payers, and patients. The inadvertent disclosures we found and documented in this report point to the larger problem facing the industry. Clearly, such hemorrhages may fuel many types of crime. While medical fraud has long been a significant problem, the crime of medical identity theft is still in its infancy. Today, many of the well-documented crimes appear to be committed out of medical need. However, with the growing opportunity to commit more significant crimes involving large financial rewards, more and more advanced schemes and methods, such as P2P-fueled identity theft, will likely develop. For criminals to profit, they don't need to "steal" an identity, but only to borrow it for a few days, while they bill the insurer carrier thousands of dollars for fabricated medical bills. This combination of medical fraud along with identity theft adds a valuable page to the playbook of thieves looking for easy targets. Stopping the supply of digital identities is one key to halting this type of illegal activity.

The Health Insurance Privacy Accountability Act (HIPAA) was created to protect patients from having sensitive medical information from becoming public or used against them. However, some of the provisions of the act make medical identity theft more difficult to track, identify, and correct. Under HIPAA, when a patient's medical record has been altered by someone else using their ID, the process to correct the record is difficult for the patient. The erroneous information in the medical file may remain for years. Also due to the intricacies of HIPAA, people who have been victims of medical identity theft may find it difficult to even know what has been changed or added to their record. Since the thief's medical information is contained within the victim's file, it is given the same privacy protections as anyone under the act. Without the ability to remove erroneous information, or figure out the changes contained in a medical record, repairing the damages of medical identity theft can be a very taxing process.

However, HIPAA is also a positive force in the fight against identity theft. Institutions have been fined and required to implement detailed corrective action plans to address inadvertent disclosures of identifiable electronic patient information (HHS 2008). In the case of Isis Machado mentioned earlier, she was charged and fined under HIPAA for disclosing individually identifiable medical records. HIPAA contains rules and punishments for offending medical professionals, which are historically the largest group of health-care fraud perpetrators. This protection of patient identities does discourage inappropriate uses of medical information and reduces the chance of hemorrhages. Nevertheless, HIPAA can do little to stop patients from disclosing their medical identities voluntarily to individuals posing as health care providers, or poorly managing their own computerized documents.

Tighter controls on patient information are a good start, but consumers still need to be educated of the dangers of lost health-care information and how to secure their information on personal computers. Hospitals and others concerned with medical identity theft have begun to undertake measures in order to curb medical identity theft. One of the simplest and most effective measures put in place by hospitals is to request photo identification for admittance to the hospital. In many cases, when a request for photo identification is made, the individual will give up on obtaining care and simply leave the hospital, never to return again. Of course, this measure will likely lose its efficacy in time as criminals become aware of the change in policy. Once a few personal identifiers have been acquired, such as date of birth and Social Security number, a criminal can obtain seemingly valid photo-ID. In the future, insurance companies may need to begin issuing their own tamper-proof photo identification to help stop medical identity theft.

Finally, health-care providers and insurers must enact better monitoring and information controls to detect and stop leaks. Information access within many health-care systems is lax. Coupled with the portability of data, inadvertent disclosures are inevitable. Better control over information access governance (Zhao and Johnson 2008) is an important step in reducing the hemorrhages documented in this report.

References

1. Ball, E., Chadwick, D.W., Mundy, D (2003), "Patient Privacy in Electronic Prescription Transfer," IEEE Security & Privacy, March/ April, 77 – 80.
2. Bolin, J.N., Clark, L.S. (2004), "Avoiding Charges of Fraud and Abuse: Developing and Implementing an Effective Compliance Program," JONA (34:12), 546 550.
3. Bosworth, M.H. (2006), "Kaiser Permanente Laptop Stolen: Personal Data on 38,000 Members Missing," Consumer Affairs, Nov 29, http://www.consumeraffairs.com/news04/2006/11/kaiser_laptop.html
4. BW (2007), "Diagnosis: Identity Theft," Business Week, January 8, 2007.
5. Claburn, T. (2007), "Minor Google Security Lapse Obscures Ongoing Online Data Risk," Information Week, January 22.
6. De Avila, J. (2007), "The Hidden Risk of File Sharing," Wall Street Journal, Nov. 7, D1.
7. Dixon, P. (2006), "Medical Identity Theft: The Information Crime that Can Kill You," The World Privacy Forum.
8. FBI (2007), "2006 Financial Crime Report" Federal Bureau of Investigation. [Online] 02 28, 2007. [Cited: 02 04, 2008.] http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm.
9. FTC (2007), "2006 Identity Theft Report," Federal Trade Commission, November, 2007, last accessed on June 18, 2008, <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>
10. Good N.S., and A. Krekelberg (2003) "Usability and privacy: a study of Kazaa P2P file-sharing," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, April 05 10.
11. Hanson, G (1994), "Illegal Aliens Bilk Sick U.S. system," Insight on the News. April 18, 1994.
12. Hendrick, B. (2008), "Insurance records of 71,000 Ga. families made public," Atlanta Journal Constitution, April 08. http://www.ajc.com/metro/content/metro/stories/2008/04/08/breach_0409.html
13. HHS (2008), "HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information," U.S. Department of Health & Human Services, News Release, July 17, <http://www.hhs.gov/news/press/2008pres/07/20080717a.html>
14. Johnson, M. E. and S. Dynes (2007), "Inadvertent Disclosure: Information Leaks in the Extended Enterprise," Proceedings of the Sixth Workshop on the Economics of Information Security, Carnegie Mellon University, June 7 8.
15. Johnson, M. E. (2008), "Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain," Journal of Management Information Systems, Vol. 25, No. 2, 97 123.
16. Johnson, M. E., D. McGuire, and N. D. Willey (2008), "The Evolution of the Peer to Peer File Sharing Industry and the Security Risks for Users," Proceedings of HICSS 41, International Conference on System Sciences, IEEE Computer Society, Jan 7-10, Hawaii.
17. Johnson, M. E., McGuire, D., and N. D. Willey (2009), "Why File Sharing Networks Are Dangerous," Communications of the ACM, 52, 2, 134 138.
18. Lafferty, L. (2007), "Medical Identity Theft: The Future Threat of Health Care Fraud Is Now," Journal of Health Care Compliance; Jan/Feb, 9, 1, 11 20.
19. Levitz, J. and J. Hechinger (2006), "Laptops Prove Weakest Link in Data Security," Wall Street Journal, March 26.
20. Mennecke, T. (2006), "Slyck News P2P Population Continues Climb," June 14, <http://www.slyck.com/news.php?story=1220>.

21. Messmer, E. (2008), "Health Care Organizations See Cyberattacks as Growing Threat," *Network World*, February 28.
22. Musco, T. D. and K. H. Fyffe (1999), "Health Insurers' Anti-fraud Programs," Washington D.C. Health Insurance Association of America.
23. Nakashima, E. and R. Weiss (2008), "Patients' Data on Stolen Laptop," *Washington Post*, March 24, A1.
24. Olson, P. (2006), "AOL Shoots Itself in the Foot," *Forbes*, August 8.
25. PA (2006), "Pennsylvania Attorney General. Attorney General's Insurance Fraud Section charges former SEPTA employee with using co-worker's ID to obtain Viagra." Harrisburg: s.n., July 6, 2006.
26. Peterson, M. (2000), "When Good Drugs Go Gray; Booming Underground Market Raises Safety Concerns," *The New York Times*, 12 14, 2000, p. 1.
27. Reavy, P. (2006), "What Baby? ID victim gets a jolt," *Deseret News* (Salt Lake City). May 2, 2006.
28. Robenstein, S. (2008), "Are Your Medical Records at Risk?" *Wall Street Journal*,
29. Russell, J. (2005), "Harvard fixing data security breaches: Loophole allowed viewing student prescription orders" *Boston Globe*, January 22.
30. Tokars, L. (2008), "Memorial Hospital loses laptop containing sensitive employee data," *WSBT*, Feb 7, <http://www.wsbtc.com/news/local/15408791.html>
31. Totty, M. (2007), "Security: How to Protect Your Private Information," *Wall Street Journal*, January 29. R1.
32. Twedt, S. (2007), "UPMC patients' personal data left on Web," *Pittsburgh Post-Gazette*, April 12.
33. USDC (2006), "United States of America vs. Fernando Ferrer, Jr. and Isis Machado," 06-60261, s.l., United States District Court Southern District of Florida, September 7, 2006.
34. USDJ (2007), "US Department of Justice. Six Indicted for Health Care Fraud Scheme in Southeast Texas," Houston, TX : s.n., 2007. Press Release.
35. USA (2007), "United States Attorney, District of Nevada. "Las Vegas Pharmacist Charged with Health Care Fraud and Unlawful Distribution of Controlled Substances," Las Vegas, United States Department of Justice, 2 23, 2007.
36. Useem, J. (2007), "Fortune 500: The Big Get Bigger," *Fortune Magazine*, 155, 8, April 30, 81. *Wall Street Journal*, March 26.
37. Vijayan, J. (2007), "Personal data on 17,000 Pfizer employees exposed; P2P app blamed," *Computer World*.
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024491>
38. Wereschagin, Mike (2006), "Medical ID Theft Leads to Lengthy Recovery." *Pittsburgh Tribune-Review*, 10 24, 2006.
39. WFTV (2008), "Medical Center Patient Records Posted On Internet," August 14, <http://www.wftv.com/news/17188045/detail.html?taf=orlc>
40. Zhao, X. and M. E. Johnson (2008), "Information Governance: Flexibility and Control through Escalation and Incentives," *Proceedings of the Seventh Workshop on the Economics of Information Security*, Dartmouth College, June 26-27.

Testimony Before the House Subcommittee on Commerce, Trade and Consumer Protection

Robert Boback, CEO, Tiversa, Inc.

May 4, 2009

TIERSA.

Good afternoon Chairman Rush, Ranking Member Radanovich and Distinguished Members of the Subcommittee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

As P2P file sharing risk continues to be a major security, risk and privacy issue, let me first start by first providing a brief background on peer to peer.

It is important to note that the Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer to Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer to Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

Peer to peer networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

The use of P2P has evolved and is used by individuals world wide for many different purposes including:

- 1 Planned file sharing its intended use.
- 2 Searching for information with malicious intent person al information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 Distribution and sharing of illegal information Child pornography and information that could be used in terror activity.

P2P networks continue to grow in size and popularity due to the alluring draw of the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie

and music files, millions of documents, that were not intend ed to be shared with others, are also available on these net works. It is this that we refer to as inadvertent sharing or dis closure.

Inadvertent sharing happens when computer users mistaken ly share more files than they had intended. For example, they may only want to share their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have adequately highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child down loads a P2P software program on his/her parents computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confiden tial or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software program variants that Tiversa has identified being used to access these net works. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program.

This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti virus programs do not detect the presence of such malicious software as it appears to the detection software as an intentionally downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, and foreign intelligence worldwide.

Today, we would like to provide the committee with concrete examples that show the extent of the security problems that are present on the P2P networks and implications of sharing this type of information. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

Despite the tools that P2P network developers are putting into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as firewalls, encryption, port scanning, policies, etc, simply do not effectively mitigate peer to peer file sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the

dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05 007 Risks of File Sharing Technology Exposure of Sensitive or Personal Information clearly states:

"By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information they will not.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers in previous hearings, the problem continues to exist. In fact, we will also seek to demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been architected in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file sharing network. Tiversa can see and detect all the previ

ously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Financial Fraud

In an analysis of these searches, listed below is a small sampling of actual searches issued on P2P networks brief research window in March 2009. The term credit card was used as the filter criteria for the period.

2007 credit card numbers
2008 batch of credit cards
2008 credit card numbers
a&l credit card
aa credit card application
abbey credit cards
abbey national credit card
ad credit card authorization
april credit card information
athens mba credit card payment
atw 4m credit card application
austins credit card info
auth card credit
authorization credit card
authorization for credit card
authorize net credit card
bank and credit card informati
bank credit card
bank credit card information
bank credits cards passwords
bank numbers on credit cards
bank of america credit cards
bank of scotland credit card
bank staffs credit cards only
barnabys credit card personal
bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their

tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases where accountant and tax offices, themselves, are inadvertently disclosing client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately \$35. This is up from approximately \$8 \$10 only a few short years ago. One plausible explanation for rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSN. This is a very important point. Our search data shows that thieves in fact a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W 2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her tax return, it will automatically be rejected by the IRS's system as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W 2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims only to have the initial victim left to address the problem with the IRS. This is very costly and time consuming to resolve.

Stolen SSNs are also used by illegal aliens as a requirement of their gaining employment here in the United States. This crime has far reaching implications as well as a tremendous tax burden on behalf of the victim.

Medical Fraud

Medical information is also being sought after on P2P networks with alarming regularity. Listed below are some terms issued over the same period regarding medical information.

letter for medical bills
letter for medical bills dr
letter for medical bills etmc
letter re medical bills 10th
ltr client medical report
ltr hjh rosimah medical
ltr medical body4life
ltr medical maternity portland
ltr medical misc portland
ltr orange medical head center
ltr to valley medical
lytec medical billing
medical investigation
medical journals password
medical.txt

medical abuse records
medical abuse
medical abuse records
medical algorithms
medical authorization
medical authorization form
medical authorization
medical benefits
medical benefits plan chart
medical billing
medical billing
medical bill
medical biller resume
medical billing software
medical billing
medical billing windows

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, he or she would then immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which he or she would quickly turn into cash by selling the drugs. This is a very difficult crime to detect as most consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company which only serves to prolong the activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

Searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. In the full year of 2006 and 2007, the average annual rise in the search totaled just over 10%.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings in this testimony would put these corporations at further risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information.

The only correlation that we identified is that the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Child Predation

As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can become even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program.

Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

Examples to follow on subsequent pages...

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|------|----------|----------|---|---|---|---|-------------|------|--------|----------|-------|---|---|--------|
| 9117 | HOSPITAL | BARBARA | | | | | NEW YORK | 7600 | Female | 12/21/58 | | | | 537.3 |
| 9118 | HOSPITAL | MARCEL | | | | | BRIDGE CITY | 7511 | Female | 10/21/54 | | | | 786 |
| 9119 | HOSPITAL | PAMELA | | | | | BRIDGE CITY | 7511 | Female | 8/29/54 | | | | 786.8 |
| 9120 | HOSPITAL | MATTHEW | | | | | BRIDGE CITY | 7511 | Male | 6/28/50 | | | | 831.48 |
| 9121 | HOSPITAL | JAMES | | | | | HIGH BLAND | 7502 | Male | 3/21/58 | | | | 782.8 |
| 9122 | HOSPITAL | WILLIAM | | | | | DALLAS | 7520 | Male | 11/21/53 | VR 3 | | | 782.8 |
| 9123 | HOSPITAL | BARBARA | | | | | PORT ARTHUR | 7802 | Female | 12/21/50 | | | | 271.85 |
| 9124 | HOSPITAL | BRENT | | | | | MIAMI | 7520 | Male | 4/21/57 | | | | 780.8 |
| 9125 | HOSPITAL | BERNARD | | | | | BRAND PRAN | 7520 | Female | 7/21/54 | | | | 282.75 |
| 9126 | HOSPITAL | MIAMI | | | | | DALLAS | 7520 | Male | 8/21/58 | | | | 789 |
| 9127 | HOSPITAL | JAMES | | | | | PORT ARTHUR | 7802 | Male | 12/21/57 | VR 0 | | | 780.8 |
| 9128 | HOSPITAL | JOHNNY | | | | | MIAMI | 7520 | Male | 12/21/56 | | | | 481.75 |
| 9129 | HOSPITAL | JOHNNY | | | | | DALLAS | 7520 | Male | 12/21/56 | | | | 281.57 |
| 9130 | HOSPITAL | GARY | | | | | BRIDGE CITY | 7511 | Male | 11/11/56 | | | | 611.15 |
| 9131 | HOSPITAL | STEVEN | | | | | GRAND | 7520 | Male | 11/21/54 | | | | 8.8 |
| 9132 | HOSPITAL | GARDEN | | | | | DALLAS | 7520 | Female | 4/21/56 | | | | 386.8 |
| 9133 | HOSPITAL | GREGORY | | | | | PORT ARTHUR | 7802 | Male | 2/21/58 | | | | 553.8 |
| 9134 | HOSPITAL | DAVID | | | | | HOUSTON | 7520 | Male | 11/21/56 | | | | 281.8 |
| 9135 | HOSPITAL | SHARMA | | | | | GRAND | 7520 | Female | 8/21/58 | | | | 271.85 |
| 9136 | HOSPITAL | MICHAEL | | | | | PORT ARTHUR | 7802 | Male | 10/21/58 | | | | 271.85 |
| 9137 | HOSPITAL | ROSEMARY | | | | | BRIDGE CITY | 7511 | Male | 8/21/56 | | | | 281.75 |
| 9138 | HOSPITAL | YOLANDA | | | | | DALLAS | 7520 | Female | 10/21/58 | VR 83 | | | 281.75 |
| 9139 | HOSPITAL | JOE | | | | | DALLAS | 7520 | Male | 2/21/57 | | | | 411.85 |
| 9140 | HOSPITAL | ROSE | | | | | DALLAS | 7520 | Female | 10/21/58 | | | | 382.8 |
| 9141 | HOSPITAL | ETTY | | | | | HOUSTON | 7520 | Female | 2/21/58 | | | | 281.8 |
| 9142 | HOSPITAL | ROSEMARY | | | | | GRAND | 7520 | Female | 8/21/58 | | | | 281.8 |
| 9143 | HOSPITAL | ELVIRA | | | | | PORT ARTHUR | 7802 | Female | 6/21/56 | | | | 281.85 |
| 9144 | HOSPITAL | HENRY | | | | | MIAMI | 7520 | Male | 2/21/56 | | | | 281.85 |
| 9145 | HOSPITAL | MICHAEL | | | | | DALLAS | 7520 | Female | 8/21/58 | | | | 381 |
| 9146 | HOSPITAL | MARY | | | | | PORT ARTHUR | 7802 | Male | 8/21/56 | | | | 281.8 |
| 9147 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Male | 11/21/58 | | | | 381 |
| 9148 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9149 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9150 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9151 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9152 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9153 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9154 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9155 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9156 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9157 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9158 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9159 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9160 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9161 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9162 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9163 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9164 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9165 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9166 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9167 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9168 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9169 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9170 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9171 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9172 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9173 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9174 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |
| 9175 | HOSPITAL | LEON | | | | | PORT ARTHUR | 7802 | Female | 11/21/58 | | | | 381 |
| 9176 | HOSPITAL | LEON | | | | | GRAND | 7520 | Male | 2/21/58 | | | | 381 |

| | A | B | C | D | E | F | G | H |
|------|-------------|-------------|-----|----------|-------------|----------------------------|-------------------|-----------|
| 4 | Last | First | SSN | Taxable? | Degree | School | Major | Division |
| 1000 | John | John | | N | Certificate | CFA Institute | CFA | Eastern |
| 1001 | Zishan | Zishan | | N | Graduate | NYIT | MBA | Western |
| 1002 | David | David | | N | Certificate | CFA Institute | CFA | Western |
| 1003 | Anthony | Anthony | | N | Graduate | Stevens Institute | MIS | Eastern |
| 1004 | Melissa | Melissa | | N | Certificate | Dowling College | CFP | Eastern |
| 1005 | Thomas | Thomas | | N | Certificate | Pace | CFP | Eastern |
| 1006 | Mary Linley | Mary Linley | | N | Certificate | American College | CFP | Eastern |
| 1007 | Samuel | Samuel | | N | Certificate | Kaplan University | CFP | Eastern |
| 1008 | Sandeep | Sandeep | | N | Graduate | Steven Institute | Info Mgmt sys | Eastern |
| 1009 | Emmee | Emmee | | N | Certificate | Kaplan | CFP | SouthWest |
| 1010 | Scott | Scott | | N | Certificate | Kaplan | CFP | Western |
| 1011 | Darya | Darya | | N | Undergrad | Montclair State University | Marketing | Eastern |
| 1012 | Isaac | Isaac | | N | Certificate | Pace University | CFP | Eastern |
| 1013 | Sofland | Sofland | | N | Certificate | Kaplan | CFP | Eastern |
| 1014 | James | James | | N | Certificate | Kaplan | CFP | Eastern |
| 1015 | Steven | Steven | | N | Graduate | University of Connecticut | MBA | Eastern |
| 1016 | Michael | Michael | | N | Graduate | Stevens Ins | MIS | Eastern |
| 1017 | Alejandra | Alejandra | | N | Degree | Pace University | BA | Eastern |
| 1018 | Hasan | Hasan | | N | Undergrad | NYU | International MBA | Eastern |
| 1019 | Sneh | Sneh | | N | Undergrad | Stevens Institute | MIS | Eastern |
| 1020 | Luis | Luis | | N | Undergrad | Axa College | BA | Eastern |
| 1021 | Jared | Jared | | N | Certificate | Kaplan | CFP | Eastern |
| 1022 | Mathew | Mathew | | N | Undergrad | Brooklyn College | Finance | Eastern |
| 1023 | Francisco | Francisco | | N | Certificate | CFA Institute | CFA | Eastern |
| 1024 | Belinda | Belinda | | N | Undergrad | Universidad | Accounting | PR |

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| 1 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| 1001 | 1002 | 1003 | 1004 | 1005 | 1006 | 1007 | 1008 | 1009 | 1010 | 1011 | 1012 | 1013 | 1014 | 1015 | 1016 | 1017 | 1018 | 1019 | 1020 | 1021 | 1022 | 1023 | 1024 | 1025 | 1026 |
| 1027 | 1028 | 1029 | 1030 | 1031 | 1032 | 1033 | 1034 | 1035 | 1036 | 1037 | 1038 | 1039 | 1040 | 1041 | 1042 | 1043 | 1044 | 1045 | 1046 | 1047 | 1048 | 1049 | 1050 | 1051 | 1052 |

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| 1053 | 1054 | 1055 | 1056 | 1057 | 1058 | 1059 | 1060 | 1061 | 1062 | 1063 | 1064 | 1065 | 1066 | 1067 | 1068 | 1069 | 1070 | 1071 | 1072 | 1073 | 1074 | 1075 | 1076 | 1077 | 1078 |
| 1079 | 1080 | 1081 | 1082 | 1083 | 1084 | 1085 | 1086 | 1087 | 1088 | 1089 | 1090 | 1091 | 1092 | 1093 | 1094 | 1095 | 1096 | 1097 | 1098 | 1099 | 1100 | 1101 | 1102 | 1103 | 1104 |
| 1105 | 1106 | 1107 | 1108 | 1109 | 1110 | 1111 | 1112 | 1113 | 1114 | 1115 | 1116 | 1117 | 1118 | 1119 | 1120 | 1121 | 1122 | 1123 | 1124 | 1125 | 1126 | 1127 | 1128 | 1129 | 1130 |
| 1131 | 1132 | 1133 | 1134 | 1135 | 1136 | 1137 | 1138 | 1139 | 1140 | 1141 | 1142 | 1143 | 1144 | 1145 | 1146 | 1147 | 1148 | 1149 | 1150 | 1151 | 1152 | 1153 | 1154 | 1155 | 1156 |

Emp No: [] Employer: [] Local: 952 Dist: 03 Paid Thru: Jul/1987
 Name: WANDA Gender: F Exp Date: 05/21/1942
 Address: [] CA
 Phone: [] Fax: [] Vol/Reg: No SA: 065 Mail: []
 Initials: 01/13/1977 Service: 08/01/1980 Death: [] Salary: \$13.00
 Rank/Rate: [] Hire: [] Term of: [] Term Exp: 01/15/1987
 Due Rate: \$26.00 Non Ann: \$26.00 Due Tvg: [] Due Let: 06/15/1987
 In Rate: \$100.00 In PD: \$100.00 Start: [] Dep: []
 Fren Rate: \$0.00 Fren PD: \$0.00 Orig: Oct/1977 Lock: []
 Beneficiary: [] Rating: 3 Kot: 010 Trust Rate: \$0.00
 Transfer To: [] From: [] No 2: [] Transf Paid: \$0.00
 Remarks: TERM 1-87 WATCH
 Access: 1 [] 2 [] 3 [] 4 [] Fnd Flag: [] Post Date: []
 Payer: [] Payee: [] PAYMENTS
 Record: 69495 of 69495

Insurance Aging

INCORPORATED

JOHN J. [] Date of Birth: 0/28/1945 Insured: Self

Insurance: Primary ID: []

| | | | | | | | | | |
|-----------------------|------------|--------|------|------|------|------|--------|--------|------|
| | 05/01/2006 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| | 12/17/2006 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| | 04/30/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | 220.00 | 0.00 | 0.00 | 0.00 | 0.00 | 220.00 | 220.00 | |

| | | | | | | | | | |
|-------------------------|--------|------|------|------|--------|--------|--------|--|--|
| Insurance Total: | 379.15 | 0.00 | 0.00 | 0.00 | 147.75 | 231.40 | 379.15 | | |
|-------------------------|--------|------|------|------|--------|--------|--------|--|--|

TIMOTHY L. [] Date of Birth: 02/21/1945 Insured: Self

Insurance: Primary Group Number: 00001022 ID: []

| | | | | | | | | | | |
|-----------------------|------------|-------------|------------|-------|------|------|------|------|-------|-------|
| 219464 | 02/17/2006 | 87088/87088 | 03/09/2006 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| | 05/13/2006 | | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| | 12/03/2006 | | | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | | | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |

DANNY T. [] Date of Birth: 01/15/1948 Insured: Self

Insurance: Primary Group Number: 00009005 ID: []

| | | | | | | | | | | |
|-----------------------|------------|-------------|------------|-------|------|------|------|------|-------|-------|
| 233355 | 05/16/2006 | 87088/87088 | 08/09/2006 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| Patient Total: | | | | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |

| | | | | | | | | | |
|-------------------------|-------|------|------|------|------|------|-------|-------|--|
| Insurance Total: | 82.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 82.00 | 82.00 | |
|-------------------------|-------|------|------|------|------|------|-------|-------|--|

BEN [] Date of Birth: 11/28/1915 Insured: Self

Insurance: Secondary ID: []

Tiversa engaged in research involving over 30,000 consumers and found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the last 60 days (2/25 4/26), Tiversa has downloaded 3,908,060 files that have been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheet sheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. Its important to note that these files were only downloaded with general industry terms and client filters running. Much more exists on the network in a given period of time.

This risk also extends to the military and to overall national security. Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of in excess of 200,000 of our troops.

This issue poses a national security risk. In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the Wall Street Journal printed a front cover story that indicated that former Pentagon officials had indicated that spies had downloaded plans for the \$300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Recommendations

Tiversa's focus has been working for several years with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and

protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

Awareness should extend to corporations as well. With consumers being asked to provide PII to employers, banks, accountants, doctors, hospitals, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary state to state and, in our experience, are seldom respected or followed by organizations.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. The breach law will also need to be enforced as many of the disclosing companies disregard the current state laws, if any to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the file name and meta data.

Military Personnel Disclosures

Congress should vigorously act to protect the safety and identity of our men and women in uniform. Soldiers who have had their information disclosed should be provided comprehensive identity theft protection services so as to prevent and guard against the use of the breached information.

National Security Disclosures

P2P networks should be continuously monitored globally for the presence of any classified or confidential information that could directly or indirectly affect the safety or security of our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it)

Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask!

Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service

Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The subcommittee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify here today.



TIVERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940 9030 *office*
(724) 940 9033 *fax*
www.tiversa.com

Testimony before the House Committee on Oversight and Government Reform

Robert Boback, CEO, Tiversa, Inc.

July 29, 2009

TI ERSA.

EXHIBIT - D

Good morning Chairman Towns, Ranking Member Issa and Distinguished Members of the Committee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

P2P file-sharing continues to be a major security risk and privacy issue. Today, I will provide a brief background on P2P networks, highlight the risks of inadvertent file sharing, provide examples of P2P file disclosures and the impact on consumers, businesses, government, the military and national security, and share our observations and recommendations.

Background: Peer-to-Peer Networks

The Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

P2P networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The P2P networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

P2P networks are growing and dynamic. Since 2005, P2P networks have grown at the rate of over 20% (CAGR). Today, worldwide P2P networks may have over 20 million users at any point in time. P2P networks are ever-changing as users join and exit constantly. The number of P2P programs or "clients" has grown to over 225, with many having multiple versions in use. Additionally, many of the

programs are open source and, accordingly, subject to modification as users see fit. P2P networks are a worldwide phenomenon with users across wide ranges of ages, educational backgrounds and incomes.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

- 1 – Planned file sharing – its intended use.
- 2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

Inadvertent File Disclosure

P2P networks continue to grow in size and popularity due to the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this unintentional sharing that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may want to share only their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads P2P software program on his/her parents' computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

Today, we will provide the Committee with concrete examples that show the extent of the security problems that exist on the P2P networks and the implications of sharing this type of information. During our testimony, we will provide the Committee with examples that illustrate the types of sensitive information available on P2P networks, provide examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers and government agencies in previous hearings, the problem remains. In fact, we will also demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Tiversa and Its Technology

Beginning in 2003, Tiversa developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been designed, developed and implemented in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, more than the number of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Tiversa uses this technology to provide P2P security and intelligence services to businesses, consumers and law enforcement agencies. The following examples demonstrate how inadvertent breaches affect individual consumers, businesses, government, military and national security and are based on our unique perspective on P2P networks.

Examples: Inadvertent Disclosures on P2P

Consumers

Financial Fraud – From analysis of P2P searches, listed below is a small sampling of actual searches issued on P2P networks during a brief research window in March 2008. The term *credit card* was used as the filter criteria for the period.

- 2007 credit card numbers
- 2008 batch of credit cards
- 2008 credit card numbers
- a&i credit card
- aa credit card application
- abbey credit cards
- abbey national credit card
- ad credit card authorization
- april credit card information
- athens mba credit card payment
- atw 4m credit card application
- austins credit card info
- auth card credit
- authorization credit card
- authorization for credit card
- authorize net credit card
- bank and credit card informati
- bank credit card
- bank credit card information
- bank credits cards passwords
- bank numbers on credit cards
- bank of america credit cards
- bank of scotland credit card
- bank staffs credit cards only
- barnabys credit card personal
- bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January of this year for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases in which accountants and tax offices, themselves, inadvertently disclosed client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately \$35 each. This is up from approximately \$8-\$10 only a few short years ago. One plausible explanation for the rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSNs. This is a very important point. Our search data shows that thieves in fact employ a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her legitimate tax return, it will automatically be rejected by the IRS as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims leaving the initial victim to address the problem with the IRS. This is very costly and time consuming for both the victim and the IRS.

Stolen SSNs are also used by illegal aliens to gain employment in the United States. This crime has far reaching implications as well as placing a tremendous tax burden on the victim.

Medical Fraud – Medical information is also being targeted on P2P networks with alarming and increasing regularity. Listed below are some terms issued over the same period regarding medical information.

- *letter for medical bills*
- *letter for medical bills dr*
- *letter for medical bills etmc*
- *letter re medical bills 10th*
- *ltr client medical report*
- *ltr hjh rosimah medical*
- *ltr medical body4life*
- *ltr medical maternity portland*
- *ltr medical misc portland*
- *ltr orange medical head center*
- *ltr to valley medical*
- *lytec medical billing*
- *medical investigation*
- *medical journals password medical .txt*
- *medical abuse records*
- *medical abuse*
- *medical abuse records*
- *medical algorithms*

- *medical authorization*
- *medical authorization form*
- *medical authorization*
- *medical benefits*
- *medical benefits plan chart*
- *medical billing*
- *medical billing*
- *medical bill*
- *medical biller resume*
- *medical billing software*
- *medical billing*
- *medical billing windows*

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, the thief would immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which can be quickly sold for cash. This is a very difficult crime to detect as many consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company, prolonging the criminal activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for valid medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

User-issued P2P searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. For the years of 2006 and 2007, the average annual rise in the search totaled just over 10%.

Child Predation – As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can be even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos

TI ERSA.

144 Emeryville Drive
Suite 200
Cranberry Township
Pennsylvania 16746

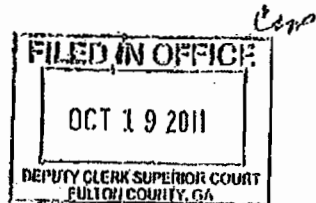
(724) 940-9030 office
(724) 940-9033 fax
www.tlversa.com



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

1.

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,

2

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 hererin.

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 Defendants' position as Director of the McNamee 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

LimeWire. 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 275,000 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 PII and/or PHI, 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.¹

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.

¹ 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 HE 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 File 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 44th 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:

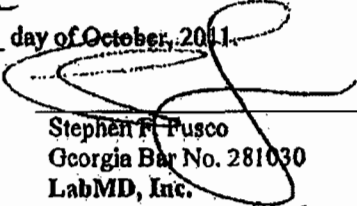
- (a) Judgment against Defendants as outlined herein;
- (b) Damages in an amount to be determined at trial;
- (c) Exemplary damages in an amount to be determined at trial.
- (d) Attorney's fees and costs associated with this litigation;
- (e) A trial by jury on the issues outlined herein;
- (f) All such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

proper.

2 p e

[SIGNATURE CONTINUE ON NEXT PAGE]

Respectfully submitted this 7 day of October, 2011.



Stephen F. 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.

**FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL
DAUGHERTY**

PETITION EXHIBIT 5

**Michael Daugherty's Petition to Limit or Quash the
Civil Investigative Demand (Jan. 10, 2012)**

(Public Version)

Table of Contents

| | <u>Page</u> |
|--|-------------|
| I. FACTUAL SUMMARY | 1 |
| A. The 1,718 File Was Illegally Downloaded By Tiversa, Inc., A Technology Corporation Using Patented Computer Technology, With The Support Of Federally-Funded Researchers At Dartmouth College | 2 |
| B. LabMD's Lawsuit Against Tiversa and Dartmouth College | 4 |
| II. ARGUMENT | 5 |
| A. The FTC's Authority Under Section 45..... | 5 |
| B. There Is No Basis Under Section 45 To Support Enforcement Of The Present CID, Which Is In All Events Exceedingly Overbroad And Unduly Burdensome | 7 |
| C. The CID Should Be Quashed Because It Is Not Authorized by A Valid Resolution And Is Therefore Indefinite, Overbroad, And Incapable Of Demonstrating A Valid Exercise Of The FTC's Section 45 Authority..... | 10 |
| D. The CID Improperly Demands Documents And Testimony Concerning Matters That Are Primarily Regulated By The Department Of Health And Human Services | 12 |
| III. CONCLUSION..... | 13 |

**MICHAEL DAUGHERTY'S PETITION TO QUASH
THE CIVIL INVESTIGATIVE DEMAND**

Petitioner Michael Daugherty, in his capacity as president of LabMD, Inc., hereby petitions the Federal Trade Commission ("FTC"), pursuant to 16 C.F.R. § 2.7(d), to quash the Civil Investigative Demand ("CID") issued to Petitioner on December 21, 2011. The FTC issued the CID pursuant to its alleged authority under Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1 and therein makes various demands, including the production of all documents related to any "security risk, vulnerability, and incidents through which [Petitioner's] documents and information [] either were or could have been disclosed to unrelated third parties."¹ Petitioner respectfully submits that the FTC lacks the authority to issue the CID in its entirety. Accordingly, Petitioner respectfully petitions the Commission to quash the CID.²

I. FACTUAL SUMMARY

Petitioner is the president of LabMD, and the present CID was issued to Petitioner in his capacity as LabMD's president. Although the CID is worded in the broadest possible manner, it appears to be premised on the third-party download of a single document belonging to LabMD, Inc. (the "1,718 File"). The 1,718 File, which contained personally identifiable information ("PII") and protected health information ("PHI") about some of LabMD's patients, was illegally downloaded from LabMD's computers in February of 2008. To Petitioner's knowledge, no other incidents such as this have occurred, nor does the CID reference or allege any additional incidents (despite the absence of any limitation to the CID's testimonial and documentary

¹ A true and correct copy of the December 21, 2011 Civil Investigative Demand is attached hereto as Exhibit A.

² This petition to quash is based on the FTC's lack of authority to issue a CID to LabMD on the basis of the 1,718 File incident. However, Petitioner explicitly reserves any and all arguments or claims concerning the CID itself in the event that the FTC is found to have the requisite authority to issue a CID targeting LabMD on the basis of the 1,718 File incident.

requests). Therefore, and because there is no other conceivable basis for the CID, Petitioner sets forth the facts surrounding the 2008 download of the 1,718 File, all of which are part of the FTC's private investigation record and/or are currently being adjudicated by a federal court in a civil action that LabMD brought against the parties who illegally downloaded the 1,718 File.

A. The 1,718 File Was Illegally Downloaded By Tiversa, Inc., A Technology Corporation Using Patented Computer Technology, With The Support Of Federally-Funded Researchers At Dartmouth College

Tiversa, Inc. is a Pennsylvania Corporation who provides peer-to-peer ("P2P") intelligence services to corporations, government agencies, and individuals based on its patented EagleVision X1 technology that can monitor over 550 million computer users daily.³ On information and belief, both Tiversa and its partner, Dartmouth College, accepted federal funds from the National Institute of Standards and Technology, the United States Department of Justice, the United States of Homeland Security, and the National Science Foundation, among other governmental agencies, to develop P2P search technology. During a 2007 congressional hearing, Tiversa testified that its proprietary technology allowed it to process 300 million searches per day, or over 170 million more searches than Google was processing per day.⁴ At the same hearing, Tiversa admitted that it had downloaded computer files containing, but by no means limited to –

federal and state identification, including passports, driver's license, 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.⁵

³ See Company Overview, Website for Tiversa, <http://www.tiversa.com/about/>.

⁴ See Tiversa's July 24, 2007 testimony before the United States House of Representatives Committee on Oversight and Government Reform, a true and correct copy of which is attached hereto as Exhibit B, at 3.

⁵ *Id.* at 5.

Two years later, in April of 2009, Dartmouth College published a paper entitled *Data Hemorrhage in the Health-Care Sector*.⁶ The paper was based upon activities “conducted in collaboration with Tiversa” using Tiversa’s proprietary technology⁷ and was financially supported by a U.S. Department of Homeland Security Grant Award issued under the auspices of the Institute for Information Infrastructure Protection.⁸ According to the paper, Tiversa and Dartmouth began their project by “looking for files from top ten publicly traded health-care firms” that were available on P2P networks.⁹ As part of the initial search, Tiversa and Dartmouth manually reviewed 3,328 computer files downloaded from P2P networks, many of which contained PII and PHI.¹⁰

Following their initial search, Tiversa and Dartmouth undertook a second search (“Second Search”) lasting approximately six months.¹¹ During the Second Search, Tiversa and Dartmouth downloaded closed to four million documents, including over 20,000 medical patient records.¹² Tiversa described the evolving technology it used for the Second Search in a 2009 hearing before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection (“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

⁶ A true and correct copy of the April 2009 paper is attached hereto as Exhibit C.

⁷ *Id.* at 1.

⁸ *Id.*

⁹ *Id.* at 8.

¹⁰ *Id.* at 9-11.

¹¹ *Id.* at 11.

¹² *Id.* at 13 (referencing the 20,000 medical patient records that were downloaded); *see also* Tiversa’s May 4, 2009 testimony before the United States House of Representatives Subcommittee on Commerce, Trade and Consumer Protection, a true and correct copy of which is attached hereto as Exhibit D, at 10 (referencing the nearly four million documents that were downloaded).

P2P network in its entirety in real time.”¹³ Further, Tiversa “processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day”.¹⁴ To showcase its technology, during the hearing Tiversa, performed a “live demonstration” whereby it intentionally searched for and downloaded over 275,000 tax returns.¹⁵

On July 29, 2009, Tiversa appeared before the United States House of Representatives Committee on Oversight and Government Reform and testified further about the technology it had used to perform the Second Search.¹⁶ According to its testimony, Tiversa deployed newly developed P2P search technology that allowed it to penetrate even “the most technologically advanced” computer security despite the presence of “firewalls and encryption.”¹⁷ It was with this technology, and during the Second Search, that Tiversa and Dartmouth downloaded the 1,718 File, a copy of which Tiversa produced at the 2009 CTC hearing.¹⁸

B. LabMD’s Lawsuit Against Tiversa and Dartmouth College

Rather than agreeing to destroy its copies of the 1,718 File or explain to LabMD how it had downloaded the 1,718 File, Tiversa solicited LabMD on six occasions to purchase its security services in order to “remediate” any issues involving the 1,718 File.¹⁹ For example, on May 15, 2008, Tiversa informed LabMD that any information regarding the means by which it acquired the 1,718 File “would require a professional services agreement.”²⁰ Dartmouth,

¹³ Ex. D at 3-4.

¹⁴ *Id.* at 4.

¹⁵ *Id.*

¹⁶ A true and correct copy of Tiversa’s July 29, 2009 testimony before the United States House of Representatives Committee on Oversight and Government Reform is attached hereto as Exhibit E.

¹⁷ Ex. E at 3.

¹⁸ Ex. B at 11.

¹⁹ *See infra* note 22, Ex. F at ¶¶ 72-98.

²⁰ *Id.* at ¶ 87.

meanwhile, used federal funding to publish at least two additional papers discussing the activities leading to the download of the 1,718 File.²¹

On November 23, 2011, LabMD filed suit against Tiversa and Dartmouth alleging, among other things, computer fraud, computer crimes, conversion, and trespass.²² Tiversa, with the support of Dartmouth, was and is running an extortionist scheme whereby it uses its government-funded technology to penetrate computer networks, download confidential files, and then sell the files back to the owners under the guise of providing network security.

II. ARGUMENT

A. The FTC's Authority Under Section 45

While 15 U.S.C. § 45(a) grants the FTC the authority to investigate deceptive or unfair practices affecting commerce, this authority is not without limits. Likewise, although Congress has empowered the FTC under Section 57b-1 to issue CIDs in support of investigations undertaken pursuant to Section 45, a CID is only enforceable to the extent it rests on a legitimate exercise of Section 45 authority. In part for this reason, CIDs are not self-enforcing and the target of a CID is entitled to judicial review of a CID to prevent misuse of the FTC's statutory authority.²³

In *U.S. v. Morton Salt Co.*, the United States Supreme Court established the standard for determining when a CID should be quashed.²⁴ Although the Court enforced the decree at issue in

²¹ *Id.* at ¶¶ 100-102.

²² *LabMD Inc. v. Tiversa, Inc.*, No 1:11-cv-4044 (Nov. 30, 2011 N.D. Ga.). A true and correct copy of the Complaint is attached hereto as Exhibit F.

²³ *See, e.g., SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1024 (D.C. Cir. 1978), *cert denied*, 439 U.S. 1071 (1979) ("The federal courts stand guard, of course, against abuses of their subpoena-enforcement processes . . .") (citing *U.S. v. Powell*, 379 U.S. 48, 58 (1964) and *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186,216 (1946)); *D.R. Horton, Inc. v. Jon Leibowitz, Chairman*, No. 4:IO-CV-547-A, 2010 WL 4630210, at *2 (N.D. Tex. Nov. 3, 2010). ("As the government notes in its motion documents, the CID is not self-executing, and may only be enforced by a district court in an enforcement proceeding.")

²⁴ 338 U.S. 632 (1950).

that case, it recognized that “a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power” of the agency.²⁵ Accordingly, the Court held that agency subpoenas or CIDs should not be enforced if they demand information that is: (a) not “within the authority of the agency,” (b) “too indefinite,” or (c) not “reasonably relevant to the inquiry.”²⁶ This standard has been consistently applied by the federal judiciary.²⁷ For example, in *SEC v. Blackfoot Bituminous, Inc.*, the Court of Appeals for the Tenth Circuit confirmed that “an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”.²⁸

The costs and burdens imposed by a CID must also be considered.²⁹ An administrative agency may not use its investigative powers to go on a fishing expedition.³⁰ Rather, a CID must be based on a justifiable belief that wrongdoing has actually occurred. The Supreme Court did

²⁵ *Id.* at 652

²⁶ *Id.*

²⁷ *See, e.g., SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512 (10th Cir. 1980) (citing *Morton Salt*, 338 U.S. at 653) (confirming that “to obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”).

²⁸ *Id.* at 514; *see also Arthur Young & Co.*, 584 F.2d at 1030-31 (noting that a subpoena request must “not [be] so overbroad as to reach into areas that are irrelevant or immaterial” and that specifications must not exceed the purpose of the relevant inquiry) (internal quotation marks and citation omitted); *FTC v. Mt. Olympus Fin. LLC*, 211 F.3d 1278 (10th Cir. 2000) (“the documents requested were reasonably relevant to an inquiry clearly within the authority of the FTC”); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 471 (2d Cir. 1996) (stating that “the disclosure sought must always be reasonable”); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1993) (holding that a CID is enforceable only “if the information sought is reasonably relevant”); *FTC v. Texaco, Inc.*, 555 F.2d 862, 881 (D.C. Cir. 1977) (stating that the “the disclosure sought shall not be unreasonable”).

²⁹ *See, e.g., FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977) (a party challenging a subpoena can successfully do so on the grounds that compliance would be overly burdensome or unreasonable); *see also Phoenix Bd. Of Realtors, Inc. v. Dep't of Justice*, 521 F. Supp. 828, 832 (D. Ariz. 1981) (the government should narrow the scope of a CID when compliance may be overly burdensome).

³⁰ *See FDIC v. Garner*, 126 F.3d 1138, 1146 (9th Cir. 1997); *FTC v. Nat'l Claims Serv., Inc.*, No. S. 98-283, 1999 WL 819640, at * 1 (E.D. Cal. Feb. 9, 1999). *See also* S. Rep. 96-500 at 4, 96th Congress 1st Session (1979) (“The FTC’s broad investigatory powers have been retained but modified to prevent fishing expeditions undertaken merely to satisfy its ‘official curiosity.’”).

not equivocate in *FTC v. Am. Tobacco Co.* when it made clear that “[i]t is contrary to the first principles of justice to allow a search through all the respondents’ records, relevant or irrelevant, in the hope that something will turn up.”³¹ And, of course, the mere fact that a party has suffered a data security incident does not imply any wrongdoing on the part of the victimized party.³² That is especially so when (as here) there are no allegations that the petitioner violated any established public policy or that petitioner’s customers suffered any injury as a result of the data incident.³³

B. There Is No Basis Under Section 45 To Support Enforcement Of The Present CID, Which Is In All Events Exceedingly Overbroad And Unduly Burdensome

In the present case, there is no basis under Section 45 for imposing a highly burdensome CID upon Petitioner to investigate either 1) the download of the 1,718 File by Tiversa and Dartmouth specifically or, 2) LabMD’s data security generally. As an initial matter, Tiversa and Dartmouth’s use of government-funded, highly-proprietary, and patented technology — which according to Tiversa’s congressional testimony can penetrate even the most robust network security³⁴ — to download the 1,718 File in February of 2008 cannot conceivably amount to an unfair or deceptive practice on the part of Petitioner or LabMD. Indeed, according to Tiversa

³¹ 264 U.S. 298,306 (1924).

³² See, e.g., Holly K. Towle, Let’s Play “Name that Security Violation!”, 11 *Cyberspace Lawyer*, Apr. 2006, at 11.

³³ “Unjustified consumer injury is the primary focus of the FTC Act.” Unfairness Statement, 104 F.T.C. 949, 1073 (1984); see also *id.* at 1076 (if a public policy is not well-established, the agency will “act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury”).

³⁴ Ex. E at 3, 6, 8 (concluding that “the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies”).

itself, the security issues enabling the download of the 1,718 File were not unique to LabMD, but were common to almost every networked computer in the country.³⁵

Likewise, the FTC cannot point to any public policy existing in February of 2008 that LabMD violated, thereby enabling Tiversa and Dartmouth to download the 1,718 File. To date, the FTC has not enacted any rules or standards regarding issues associated with P2P networks, which is the FTC's most common remedy for problematic issues "that occur on an industry-wide basis."³⁶ And it was not until 2010 that the FTC began notifying organizations that failure to take adequate steps to protect against the security issues posed by P2P networks could result in liability under federal law.³⁷ 2010 was also the year in which the FTC first published *Peer-to-Peer File Sharing: A Guide for Business*.³⁸ Thus, by all accounts, the present CID seeks to hold LabMD's 2008 conduct to a standard of perfect security, a standard that the FTC itself has made clear is impossible to attain.³⁹ This is not only unfair and unreasonable, but it grossly exceeds the FTC's authority under Section 45 to investigate unfair and deceptive practices as the 2008 download of the 1,718 File by Tiversa and Dartmouth is evidence of neither.

And yet, based apparently on nothing more than possession of the 1,718 File, the CID seeks, among other things, production within 30 days of all documents relating in any manner to

³⁵ *Id.*

³⁶ A Brief Overview Of The Federal Trade Commission's Investigative And Law Enforcement Authority, July 2008, Section II(b), available at <http://www.ftc.gov/ogc/brfovrw.shtm>.

³⁷ See *FTC Warns of Breach Risk From P2P File-Sharing*, 9 No. 3 Employer's Guide HIPAA Privacy Requirements Newsl. 4 (Apr. 2010).

³⁸ Available at <http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business>.

³⁹ See Statement of the Federal Trade Commission Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations, and the Census, Comm. on Government Reform (Apr. 21, 2004) at 4 ("The Commission recognized that there is no such thing as 'perfect' security and that breaches can occur even when a company has taken all reasonable precaution."), available at <http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf>. See also Deborah Platt Majoras, *The Federal Trade Commission: Learning from History as We Confront Today's Consumer Challenges*, 75 UMKC L. Rev. 115, 128 (2006) ("The laws and rules we enforce do not require that information security be perfect. Such a standard would be costly and unobtainable.").

all of LabMD's security practices and policies (without temporal limitation). This is not only unduly burdensome, and therefore unenforceable,⁴⁰ but the overwhelming majority of documents related to LabMD's security practices and policies, past and present, have nothing to do with the 2008 download of the 1,718 File. There is absolutely no basis for using the 1,718 File download as a springboard to conduct a costly and burdensome fishing expedition into LabMD's security practices and procedures.⁴¹

The FTC's timing here is also troubling. The 2008 download of the 1,718 File was explicitly reviewed by at least two congressional committees (none of which recommended taking any course of action against LabMD). And yet, in the three years since the download of the 1,718 File was publicized in the chambers of the Congress and elsewhere, the FTC took no action. It wasn't until LabMD declined to engage Tiversa for "security services" for the sixth time and then sued Tiversa for theft and extortion that the FTC was compelled to issue the present CID. This unusual timing only serves to incentivize organizations to pay off Tiversa (as non-payment appears to coincide with the opening of an FTC investigation).

Taken together, the present CID vastly exceeds the FTC's authority under Section 45. The government funded download of the 1,718 File in 2008 by Tiversa and Dartmouth manifestly fails to provide any evidence whatsoever of any unfair or deceptive practice by LabMD. Consequently, the 1,718 File download (and the facts surrounding the download) not only does not provide a basis for a further FTC investigation into the download itself vis-a-vis

⁴⁰ See *FTC v. Texaco, Inc.*, 555 F.2d at 882 (respondent should not have "to cull its files for data" that would "impose an undue burden" and finding that a subpoena requiring production of "all documents that in any way reference" the issue in question "would be unduly burdensome").

⁴¹ When a CID makes demands "of such a sweeping nature and so unrelated to the matter properly under inquiry" such that they are not "reasonably relevant", they should not be enforced. See *Morton Salt Co.* 228 U.S. at 652; see also *In re Sealed Case (Administrative Subpoena)*, 42 F.3d 1412, 1420 (D.C. Cir. 1994) (remanding to the district court to determine whether the information requested related to a "valid purpose" of the agency's investigation).

LabMD, but it emphatically does not provide any basis for a deeply burdensome, open-ended investigation into all of LabMD's past and present security practices and procedures. As a result, the present CID should be quashed.

C. The CID Should Be Quashed Because It Is Not Authorized by A Valid Resolution And Is Therefore Indefinite, Overbroad, And Incapable Of Demonstrating A Valid Exercise Of The FTC's Section 45 Authority

Under 16 C.F.R. § 2.6, "any person under investigation compelled or requested to furnish information or documentary evidence shall be advised of the purpose and scope of the investigation and of the nature of the conduct constituting the alleged violation which is under investigation and the provisions of law applicable to such violation." Courts assess the validity of a CID by looking to the purpose and scope of the investigation and the nature of the conduct constituting the alleged violation as stated in the authorizing resolution.⁴² Importantly, however, a court can look only to the resolutions (and not any outside communications) to evaluate the scope of an investigation.⁴³ Accordingly, the FTC Operating Manual provides that –

Investigational resolutions must adequately set forth the nature and scope of the investigation. The statement may be brief, but it must be specific enough to enable a court in an enforcement action to determine whether the investigation is within the authority of the Commission and the material demanded by the compulsory process is within the scope of the resolution.⁴⁴

The single resolution that purportedly supports the present CID utterly fails the FTC's own rules and operational requirements. The resolution states, in its entirety, that "the nature and scope" of the FTC's investigation is –

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.

⁴² See, e.g., *F.T.C. v. Carter*, 636 F.2d 781,789 (D.C. Cir. 1980).

⁴³ See, e.g., *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992).

⁴⁴ O.M.3.3.6.7.4.1.

Such investigation shall, in addition, determine whether the Commission action to obtain redress of injury to consumers or others would be in the public interest.

This resolution is so sweeping that it would allow the Commission to investigate any person or entity with respect to anything. Such a broad resolution is inconsistent with both 16 C.F.R. § 2.6 and the statutory resolution requirement in 15 U.S.C. § 57b-1(i).⁴⁵

In upholding a resolution that was far more specific than the resolution here, the D.C. Circuit made clear that there are limits to the FTC's use of broad, non-specific resolutions. Under the D.C. Circuit's standard, the present resolution is utterly inadequate:

The Commission equaled this standard, and allowed our examination of the relevance of their subpoena requests, by identifying the specific conduct under investigation — cigarette advertising and promotion — and specific statutory provisions that confer authority and duties upon the Commission. Section 8(b) of the Cigarette Labeling and Advertising Act, under which the Commission must report to Congress on the effectiveness of cigarette labeling and current practices and methods of cigarette advertising and promotion, is self-expressive of several purposes of this investigation. We can therefore say that recitation of the statutory authority itself alerts the respondents to the purposes of the investigation. *Section 5's prohibition of unfair and deceptive practices, which, standing broadly alone would not serve very specific notice of purpose*, is defined by its relationship to section 8(b), as is the extremely broad and non-specific statutory authority to compile information and make reports to Congress conferred upon the Commission in section 6 of the FTC Act. The Commission additionally defined the application of section 5 in the Resolution by relating it to the subject matter of the investigation "the advertising, promotion, offering for sale, sale, or distribution of cigarettes...." We thus feel comfortably apprised of the purposes of the investigation and subpoenas issued in its pursuit, and suspect that respondents, who may feel less comfortable, are also quite aware of the purposes of the investigation.⁴⁶

Here, the bare recitation of Section 5's "prohibition of unfair and deceptive practices ...

⁴⁵ The resolution also cannot be justified as a "blanket resolution." As the FTC Operating Manual states, blanket resolutions are only appropriate "in a limited number of instances", such as to authorize second requests in antitrust investigations. O.M. 3.3.6.7.4.3.

⁴⁶ *F.T.C. v. Carter*, 636 F.2d 781,788 (D.C. Cir. 1980) (emphasis added).

stands broadly alone”. Accordingly, the resolution fails to reasonably define the nature and scope of the present investigation, and is therefore both invalid and incapable of providing the necessary support for the present CID. Consequently, the present CID should be quashed.

D. The CID Improperly Demands Documents And Testimony Concerning Matters That Are Primarily Regulated By The Department Of Health And Human Services

The CID should also be quashed because it demands documents and information concerning data security information over which the United States Department of Health and Human Services (“HHS”) has exclusive administrative and enforcement authority. As a healthcare sector corporation, LabMD was at all times relevant to the 2008 download of the 1,718 File regulated by HHS with respect to the privacy rules and patient data security requirements related to PHI under the Health Insurance Portability and Accountability Act (“HIPAA”).⁴⁷ It is undisputed that Congress gave HHS exclusive administrative and enforcement authority over data privacy and security issues.⁴⁸ As former FTC Chairman Deborah Majoras told Congress in 2005, HIPAA and its Privacy Rule are not enforced by the FTC.⁴⁹ This understanding was affirmed before Congress a year later by FTC Associate Director Joel Winston.⁵⁰ Accordingly, it is unreasonable and unduly burdensome to subject LabMD to the broad investigative demands made in the present CID as the FTC is not the primary regulator of data privacy and security issues in the healthcare sector, and unlike HHS, the FTC does not have

⁴⁷ 45 C.F.R. § 160.300 *et seq.*

⁴⁸ See 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000).

⁴⁹ Deborah Platt Majoras, Chairman of the Federal Trade Commission, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*, a prepared statement before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs (Mar. 10, 2005).

⁵⁰ Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, Statement of Joel Winston, a prepared statement before the U.S. House of Representatives, Subcommittee on Social Security of the House Committee on Ways and Means (Mar. 30, 2006).

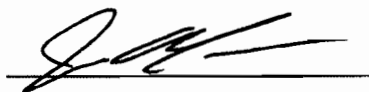
the Congressionally-delegated administrative or enforcement powers (or responsibilities) concerning these issues.

Consequently, the present CID improperly inserts the FTC into what is squarely the regulatory jurisdiction of HHS without providing any legal or policy justification for doing so. A regulated entity like LabMD is entitled to one consistent set of data privacy and security regulations. By order of Congress, that set of regulations comes from HHS, not the FTC. Accordingly, the CID should be quashed.

III. CONCLUSION

Because the present CID was issued pursuant to an impermissible exercise of the FTC's Section 45 authority — namely, because there is no basis in law or fact for using the 2008 download of the 1,718 File as grounds to conduct an unbounded, undefined, highly burdensome, and purposeless investigation into LabMD's data security practices and policies, and further because such an investigation would impermissibly intrude upon the regulatory jurisdiction of a sister agency — the present CID should be quashed.

Dated: January 10, 2012

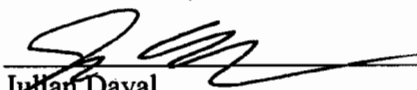


Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP
2900 K Street, NW
North Tower - Suite 200
Washington, DC 20007
Phone: (202) 625-3613
Facsimile: (202) 298-7570
Email: claudia.callaway@kattenlaw.com

Counsel for Petitioner

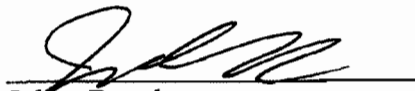
CERTIFICATION

Pursuant to 16 C.F.R. § 2.7(d)(2), counsel for Petitioner hereby certifies that counsel met and conferred with FTC counsel in a good faith effort to resolve by agreement the issues set forth in this Petition, but the parties were unable to reach agreement.


Julian Dayal

CERTIFICATE OF SERVICE

I hereby certify that on the 10th day of January, 2012, I caused the original and 12 copies of the foregoing Petition to Quash with attached exhibits to be filed by hand delivery with the Secretary of the Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, DC, 20580, and one copy of same to be filed by hand delivery with Alain Sheer, Esq., Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Avenue, N.W., Washington, D.C., 20580.


Julian Dayal

United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Michael J. Daugherty, President
LabMD Inc.
2030 Powers Ferry Road, Bld. 500, Suite 520 Atlanta, Ga 30339

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

| | |
|--|---|
| LOCATION OF HEARING | YOUR APPEARANCE WILL BE BEFORE |
| FTC - Southeast Region 225 Peachtree Street NE Suite 1500 Atlanta, Ga 30303 | Alain Sheer or other duly designated person |
| DATE AND TIME OF HEARING OR DEPOSITION | |
| JAN 23 2012 | |

You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

JAN 18 2012

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Ruth Yodanis/Kevin Havens
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

5. COMMISSION COUNSEL

Alain Sheer
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

DATE ISSUED

12/21/11

COMMISSIONER'S SIGNATURE

J. Thomas Ross

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

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



United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Michael J. Daugherty, President
LabMD Inc,
2030 Powers Ferry Road, Bld. 500, Suite 520 Atlanta, Ga 30339

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

| | |
|---|---|
| LOCATION OF HEARING FTC - Southeast Region 225 Peachtree Street NE Suite 1500 Atlanta, Ga 30303 | YOUR APPEARANCE WILL BE BEFORE Alain Sheer or other duly designated person |
| DATE AND TIME OF HEARING OR DEPOSITION JAN 23 2012 | |

You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

JAN 18 2012

3. SUBJECT OF INVESTIGATION

See attached resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Ruth Yodaiken/Kevin Havens
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

5. COMMISSION COUNSEL

Alain Sheer
Federal Trade Commission, Division of Privacy and Identity Protection
601 New Jersey Ave., NW
Mail Stop NJ-8100
Washington, DC 20001

DATE ISSUED

12/21/11

COMMISSIONER'S SIGNATURE

J. Thomas Ross

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

A copy of the Commission's Rules of Practice is available online at [http://ftc.gov/ftc/Bureaus/Practices](http://ftc.gov/ftc/ftc/Bureaus/Practices). Paper copies are available upon request.

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature _____

Title _____

Sworn to before me this day

Notary Public

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

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

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY
AND/OR DATA SECURITY**

File No. P954807

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.


Donald S. Clark
Secretary

Issued: January 3, 2008

**CIVIL INVESTIGATIVE DEMAND SCHEDULE
FOR ORAL TESTIMONY AND INTERROGATORY RESPONSE
TO MICHAEL J. DAUGHERTY**

**To: Michael J. Daugherty, President
LabMD, Inc.
2030 Powers Ferry Road
Building 500, Suite 520
Atlanta, Ga. 30339**

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

- A.** "And," as well as "or," shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in this Schedule all information that otherwise might be construed to be outside the scope of the specification.
- B.** "Any" shall be construed to include "all," and "all" shall be construed to include the word "any."
- C.** "CID" shall mean the Civil Investigative Demand, including the attached Resolution and this Schedule, and including the Definitions, Instructions, and Specifications.
- D.** "Company" shall mean LabMD, Inc., its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
- E.** "Document" shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, 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, agenda, minute, code book or label. "Document" shall also include Electronically Stored Information.
- F.** "Each" shall be construed to include "every," and "every" shall be construed to include "each."
- G.** "Electronically Stored Information" or "ESI" shall mean 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 information created,

manipulated, communicated, stored, or utilized in digital form, requiring the use of computer hardware or software. This includes, but is 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 video and sound recordings, whether stored on: cards; magnetic or electronic tapes; disks; computer hard drives, network shares or servers, or other drives; cloud-based platforms; cell phones, PDAs, computer tablets, or other mobile devices; or other storage media. "ESI" also includes such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.

H. "FTC" or "Commission" shall mean the Federal Trade Commission.

I. "Identify" shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable; and (c) documents by bates number or by title or description, date, and author.

J. "You" and "Your" shall mean Michael J. Daugherty.

K. The singular shall be construed to include the plural, and the plural shall be construed to include the singular.

II. INSTRUCTIONS

A. **Sharing of Information:** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11 (c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. **Meet and Confer:** You must contact Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127, as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your response.

C. **Applicable time period:** Unless otherwise directed in the specifications, the applicable time period for the request shall be from January 1, 2007 until the date of full and complete compliance with this CID.

D. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;
2. the names, addresses, positions, and organizations of all authors and recipients of the item; and
3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

E. Document Retention: You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. See 15 U.S.C. § 50; see also 18 U.S.C. §§ 1505, 1519.

F. Information Identification: Each interrogatory specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification(s) or sub-specification(s) to which it is responsive.

G. Petitions to Limit or Quash: Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

H. Modification of Specifications: If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with Alain Sheer, at 202.326.3321, or Ruth Yodaiken, at 202.326.2127. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

I. Procedures: This CID is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1. The taking of oral testimony pursuant to this CID will be conducted in conformity with that section and with Part 2A of the Commission's Rules, 16 C.F.R. §§ 2.8-2.9.

J. Scope of Search: This CID covers documents and information 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, other agents and consultants, and the Company, whether or not such documents and information were received from or disseminated to any person or entity.

K. Certification: You shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

III. SPECIFICATIONS

A. ORAL TESTIMONY

Subjects for testimony will include but not be limited to the following:

1. The Company's information security policies, practices, training, and procedures (collectively, the "security practices").
2. Security risks, vulnerabilities, and incidents through which Company documents and information (such as information collected from or about patients) either were or could have been disclosed to unrelated third parties (collectively, "security incidents"), including, but not limited to, P2P file-sharing applications and documents such as the [REDACTED] file (also known as [REDACTED] in Civil Action File No. 2011CV207137 filed in the Superior Court of Fulton County, Georgia).
3. The roles and responsibilities of Michael J. Daugherty, individual employees, and individual contractors in (a) developing, adopting, implementing, and monitoring the security practices, and (b) responding to security incidents.

B. INTERROGATORIES

1. Identify all documents that provide a basis for your testimony pursuant to this CID.
2. Identify all documents that you reviewed or considered in preparing to testify pursuant to this CID.

**Robert Boback
Chief Executive Officer
Tiversa, Inc.**

**Testimony Before the
House Committee on Oversight and Government
Reform**

July 24, 2007

Good morning Chairman Waxman, Ranking Member Davis and distinguished members of the committee.

My name is Robert Boback and I am Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides information technology and investigation services that help protect organizations, government agencies and individual consumers from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

I wish to extend our most sincere appreciation for inviting us to testify on this very important issue today. And I also want to applaud the Chairman for calling this important hearing and this committee's previous legislation and work on this topic.

While the Internet is a true boon to our society and economy, there are critical personal privacy and national security issues that need to be addressed seriously, urgently and with the immediate intent to find solutions.

These privacy and security threats are caused by the inadvertent misuse of P2P file sharing software, which Tiversa estimates has been installed on over 450 million computers worldwide. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the world wide web, it is not without inherent risks.

P2P technology provides an efficient way for people to share files with each other. Essentially, the technology uses the muscle power of the computers that it connects and allows people to share files directly with each other. When files are shared directly between two P2P users, this is called decentralized file sharing. This means the files do not go through any central computer server in the middle of the exchange.

P2P has gained both popularity and notoriety for the file sharing of entertainment content among its users. Yet, regardless of where one stands on P2P activity, it's unquestioned that P2P usage is rapidly growing and becoming generally accepted as the most efficient way to distribute large pieces of digital content to consumers.

Indeed, with the explosive increase in digital content including online video and user generated digital content, P2P file sharing is being embraced by many legitimate, well-known businesses to distribute and share television shows and full-length movies to consumers in a manner that protects the copyright and privacy of the content.

Therefore, P2P file sharing is becoming as much of a critical and integral part of the Internet's infrastructure as Web browsers are today. As a result, we must consider the privacy and security issues around it accordingly while allowing for legitimate uses of the technology.

Inadvertent file sharing happens when computer users mistakenly share more files than they intend. For example, they may only want to share their music files or a large academic report, but instead open all files on their computer's hard drive to access by other users on the P2P network. This typically occurs by a user error in either installing and/or using the software.

The result of inadvertent file sharing is hundreds of thousands of sensitive, confidential, and classified files are exposed and made available to the universe of P2P users each day.

Today, we would like to provide the committee with concrete examples that show the extent of how inadvertent P2P file sharing can negatively affect consumers, corporations, government entities and, indeed, our national security. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how users on P2P file sharing networks actively search for inadvertently shared sensitive information, and offer our thoughts on actions to address this problem.

Despite the tools that P2P networks are putting into their software to avoid the inadvertent file sharing of private or classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC has issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act, co-sponsored by Chairman Waxman, Ranking Member Davis and several members of this committee highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as Carnegie Mellon University's Computer Emergency Response Team (CERT) and

the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's *ST05-007-Risks of File-Sharing Technology - Exposure of Sensitive or Personal Information* clearly states:

“By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.”

Additionally, many of the most popular P2P tools prominently display similar warnings to their users.

Regardless, the problem persists, and our opinion is that it's getting worse. Here is why we hold this opinion.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can round-up all the previously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a portion of a P2P file sharing network, Tiversa can see the whole. It is our belief that no other system has this capability. We have the unique ability to observe activity across P2P networks, to see what inadvertent file sharing is taking place, and to see how P2P users are seeking this information, and where the information goes once it is shared.

Tiversa can monitor, on average, at least 300 million total P2P requests per day. We can investigate more fully to determine the intent of those requests. Our systems have the ability to record the searches for files made on P2P networks, as well as the ability to access the files available to users of P2P networks who issue these searches.

Users on a P2P networks must “ask” the network for a file before they can download them. For example, they may request “Frank Sinatra, I Did It My Way.” That search request is then broadcasted to all connected users for a response that says in effect - “I have that song”. At this point, the searcher can initiate a download request from their choice of users who possess that file.

Substitute the Sinatra search for “classified troop movements” and you begin to understand the problem. Or, if someone searches for “ABC Bank August Statement”, we can deem their intent was to obtain bank statements.

For example, Tiversa set its algorithms to record P2P search strings that matched the term “Credit Card” and separately the term “Medical.” Illustrated below is a limited set of English language examples taken from the millions of similar search strings that Tiversa observes each day:

Credit Card

| | |
|--------------------------------|----------------------------------|
| ▪ d&b credit card info | ▪ credit card pin numbers |
| ▪ corporate credit card log | ▪ credit card with cv2 numbers |
| ▪ credit card merch copy sr | ▪ credit card statements |
| ▪ davids credit card numbers | ▪ credit card comm sept private |
| ▪ credit card charge ctm costa | ▪ credit card authorisation july |
| ▪ credit card gateway ubc | ▪ credit card app pdf |
| ▪ 2007 batch of credit cards | ▪ athens mba credit card payment |
| ▪ cash credit card checks | ▪ cathys visa credit card go on |
| ▪ confidential credit card app | ▪ credit card with acc |
| ▪ credit card processing | ▪ credit card statements |

Medical

| | |
|--|-------------------------------|
| ▪ dear medical insurance my | ▪ child medical exam |
| ▪ letter re medical bills 10 th | ▪ billing medical august |
| ▪ denial of medical insurance | ▪ digital files medical trans |
| ▪ medical passwords | ▪ authorizationform medical |
| ▪ hospital records | ▪ caulfield general medical |
| ▪ comprehensive medical | ▪ medical coding and billing |
| ▪ medical release | ▪ medicine medical passwords |
| ▪ classified medical records | ▪ isilo medical |
| ▪ electronic medical record | ▪ doctors office medical exam |
| ▪ ltr medical maternity Portland | ▪ medical abuse records |

There are literally thousands of search strings that we can use to illustrate the millions of individual searches targeting sensitive information available on file sharing networks. One has to ask the question, “Why are P2P users searching for these files on a network typically used to share music and movies?” What are these users looking for? What will they do with the information once they find it?

We would now like to describe how consumers, businesses and government entities are victims of this problem by showing and describing actual examples of sensitive, confidential, and classified files inadvertently disclosed by these entities.

Individuals at Risk

P2P is a highly efficient way for a potential identity thief to gather an individual's private, privileged information that can then be used to commit ID theft, other forms of fraud, or put the individual's personal safety at risk. Yet, very few individuals are aware of this problem, let alone how to protect their information. There have been significant public awareness efforts aimed at educating consumers about phishing scams and other malicious activities. There has been very little effort made to protect consumers from inadvertently sharing information through P2P networks. Virus checking and firewalls, commonly highlighted as the solution, are not fully effective at solving inadvertent file sharing problem.

Examples of readily available documents Tiversa has been able to find on P2P file sharing networks include:

- Federal and State identification including passports, drivers licenses, and social security cards
- Dispute letters with banks, credit card companies, or insurance companies revealing account numbers, credit card numbers, insurance ID numbers and social security numbers
- Copies of individual credit check reports (e.g. Equifax Reports)
- Copies of individual bank and credit card statements
- Signed copies of health insurance cards
- Full copies of federal, state, and local tax returns
- Extensive electronic records of active usernames / ID's for online account access
- Wills and trust documents
- Mortgage and credit applications
- Life insurance applications
- Confidential medical history and records including psychiatric records
- Employment applications
- Family photographs and movies revealing children, addresses, and other personal information
- Student loan / aid applications and documents

Redacted examples that protect the privacy of individual document owners have been provided to the Committee.

In essence, whatever an individual stores on his/her computer electronically can be inadvertently shared. The impact of sharing these files not only hurts individual consumers directly, but also impacts the financial institutions, insurance firms, and government agencies who must incur the costs of fraud and investigations into wrong-doing. In these cases, consumers may hold these institutions responsible, when they themselves are exposing their own information. The lack of a mechanism to trace back to the source of the disclosure is often the issue in these cases. Fraud occurs, but consumers, corporations, and government organizations often do not know the root cause.

Corporate Breaches

Corporate inadvertent file sharing includes any entity that is not a governmental organization or an individual. No organization, regardless of its size or industry is immune from this problem. This ranges from the world's largest multi-national corporations across the financial services, insurance, defense, pharmaceutical, professional services and healthcare industries to small medical, accounting and law practices. Equally, no organizational function is immune to inadvertent file sharing. Tiversa has found files disclosed by and affecting human resources, finance, compliance, legal, research and development, sales, marketing, public relations, and the executive office.

With the increasing virtualization of corporate entities and the greater use of outsourcing, the concept of the *Extended Enterprise* has become critical to Tiversa's clients. This means that any entity entrusted with the corporations sensitive or confidential information can become a disclosure point on P2P file sharing networks. These entities include at home or virtual employees, contractors, suppliers, attorneys, consultants, accountants, or partners. These entities are almost always outside of the corporate perimeter and, therefore, outside of the direct control and enforcement of the corporation. How many times have you e-mailed a file home on which to work? Sent a confidential file to your lawyer or accountant? Inadvertent sharing over P2P file sharing networks is perfectly designed to exploit the *Extended Enterprise*. Our examples will show this.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings would put these corporations at risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information. In fact, many times we will see P2P users searching for specific file titles on a corporation. A recent example shows P2P users searching for a foreign exchange system design document for a major financial institution more than 40 times over a three week period. Tiversa knows this document is available since we obtained it as part of our work for a client.

The larger and better known a company and its brand, the greater the risks associated with searches for these corporations.

Tiversa has many examples of corporate information disclosures. Obviously, many are extremely sensitive and would put these corporations at significant risk if they were shared in a public domain. We are happy to share illustrative information with the committee in a secure environment if specific examples are needed.

The following, however, represents examples and situations that we have encountered illustrating the risk facing corporations today.

The first example illustrates a number of points relating to corporate disclosures clearly. Tiversa has discovered a third party attorney whose clients are the world's largest pharmaceutical manufacturers disclosing 436 sensitive and confidential files related those clients. The information covers, in part, pending litigation. One document, dated April 2007, is labeled "confidential" and "by hand" and addressed to Chairman Waxman with a carbon copy to Ranking Member Davis. It appears to address questions regarding drug trials of this pharmaceutical company. This is a case of an attorney who has exposed multiple pharmaceutical companies outside of their network – a clear example of extended enterprise risk.

A second case involves the exposure of the recent board minutes of one of the world's largest financial services organizations, and was disclosed by an executive assistant to one of the executive team members. This disclosure was originally found by a private investigator and reported to the corporation.

A third case involves the disclosure of the entire foreign exchange trading backbone for one of the world's largest multi-national financial firms. These files were among hundreds of confidential internal computer design and security files. As we stated earlier, P2P users were searching for these by name.

A fourth case illustrates how a contractor can expose a corporation. Tiversa observed P2P searches involving a contractor to one of our clients. Files exposed include the entire launch plan and expected growth targets for this diversified financial institution's entry into Europe. In addition, Tiversa observed these files in the possession of a P2P user in Nigeria. In this instance, a subcontractor to the initial contractor exposed our client's confidential information.

A fifth case again illustrates how a supplier can expose a corporation. Tiversa recovered the wide-area network and disaster recovery plan for a major banking institution exposed by the company to which the bank's entire trading network was outsourced.

Tiversa can provide literally hundreds of case examples like those illustrated above. In addition, we have found:

- Press releases in mark-up before their public release covering material, non-public information
- Patent related files before submission to the patent and trademark office
- Drug trial test records before FDA approval
- Legal documents including business contracts, non-disclosure agreements, term sheets, etc.
- Human resources related documents including employee reviews, executive recruiter post-interview write-ups, confidential termination and pending litigation documents, etc.
- Accounting related documents including audit reports, corporate tax records, payrolls, invoices, etc.

- Information systems related documents including administrative user ID / passwords to corporate systems, network diagrams, router access codes, functional specifications, disaster recovery plans

Highly select redacted examples that protect the privacy of individual document owners and any other sensitive information have been provided to the committee.

Given the media exposure that “lost laptops” and information disclosures on non-P2P networks has received, P2P inadvertent file sharing represents a significant brand, operational, legal, and regulatory risk to corporations. For example, a recent P2P sourced breach affecting 17,000 current and former Pfizer employees’ personal information illustrates the impact of the inadvertent sharing of sensitive information on P2P file sharing networks. Any one of the examples provided to the committee could result in a similar problem for its respective corporation.

Classified Government Data Exposed

Inadvertent P2P file sharing affects all levels and branches of government, law enforcement, and intelligence agencies. For our testimony today, Tiversa will focus on how inadvertent file sharing affects federal government agencies and law enforcement.

As with corporations, government inadvertent file sharing may originate with the agencies themselves, contractors to these agencies, soldiers or agents in the field. The same “extended enterprise” exposure problem facing corporations faces the government.

In addition, Tiversa regularly sees P2P searches for government related information including classified information and searches that could assist law enforcement.

In 2003, Chairman Waxman, Ranking Member Davis and many members of this committee co-sponsored the Government Network Security Act. It was designed to quite simply: “require Federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by peer-to-peer file sharing.”

In a press release announcing the Act, Ranking Member Davis was quoted saying, “Few people recognize these risks. Using these programs is similar to giving a complete stranger access to your personal file cabinet.”

Unfortunately, while the bill passed the House, it stalled in the Senate. Now, four years later, there are hundreds, if not thousands, of examples of federal government classified documents publicly available on P2P networks at this very moment.

A stark example is the discovery of 34 classified documents available and found by Tiversa on P2P networks. At least one of these classified examples was

related to a government contractor. At least one of the classified documents is the secret property of the United Kingdom, which shows the inadvertent release of such sensitive data is unquestionably global in nature.

Prior to our testimony today, Tiversa provided secret classified documents we located to General Wesley Clark, an equity holding member of Tiversa's advisory board. He has since furnished these documents to the Chairman of the National Intelligence Advisory Board for investigation. This information could, and most likely does, pose significant risks to our interests domestically and abroad. Unfortunately, this is not an isolated incident.

Inadvertently shared information is not limited to classified information. A diverse amount of information exists across government agencies and contractors. Here are some examples:

1. A document illustrating over 100 individual soldier's names and social security numbers
2. Physical Threat Assessments for multiple cities such as Philadelphia, St. Louis, and Miami
3. A government contractor exposing an air force base physical security attack assessment
4. A document titled "*NSA Security Handbook*"
5. A detailed report from a well known government contractor for the National Security Agency (NSA) which outlines how to connect two secure DoD networks
6. Numerous Department of Defense Directives (DoDD's) on various Information Security topics – all signed by various Assistant and Deputy Secretaries of State
7. Various Department of Defense Information Security system audits, reviews, procedures, etc. (e.g. retina scanner equipment audits, penetration detection software/equipment reviews)
8. Numerous "Field Security Operations" documents including router checklist procedures, "Network Infrastructure Security Checklist", etc.
9. Numerous presentations for Armed Forces leadership on various Information Security topics including how to profile "hackers" and potential internal information leakers
10. Large numbers of army documents marked "For Official Use Only"

A case example illustrates the risks clearly. On July 17, 2007, Tiversa found a defense contractor employee disclosing 1,900 individual files from one IP address on P2P file sharing networks. This contractor supports 34 "Joint and Army agencies", including the Department of Defense at the Pentagon, Defense Intelligence Agency, National Security Agency, US Air Force, Army, Navy and the National Imagery and Mapping Agency. This person was disclosing a wide array of files including music, personal information, resumes, photos, etc. Alarming, this individual was also disclosing 534 files with extremely sensitive, privileged information regarding the US Government generally, and the Department of

Defense and various US Armed Forces specifically. The types of information disclosed included:

- The entire Pentagon secret backbone network infrastructure diagram including server/IP addresses
- Password change scripts for Pentagon secret network servers
- Department of Defense employees contact information (including cell and home phone numbers)
- Secure Sockets Layer (SSL) instructions and certificates allowing access to the disclosing contractors' IT systems
- A contract issued by the "Army Contracting Agency" at the Pentagon that authorizes expenditures in excess of \$1.5 million with the disclosing contractor
- Numerous policies/procedures regarding the Pentagon's IT infrastructure as well as its threat response activities (including a "Draft Strategic Plan" for 2007 – 2011)
- A letter from a "Deputy Director for Management" at the "Executive Office of the President's Office of Management and Budget" which explicitly talks about some of the risks associated with P2P file sharing networks.

Ironically, it appears that the individual disclosing this information could be a member of a computer incidence response team and could hold top secret clearance – certainly not an uninformed computer user.

The risks posed by this disclosure source are widespread. For one, the disclosed information could be used directly to penetrate the Pentagon's secure IT environment in an effort to access highly classified information. Secondly, the information could be used indirectly against the disclosure source for blackmail, coercion, kidnapping, etc.

Outside of the alarming nature of this instance, this case clearly illustrates a number of key points:

- Extended Enterprise Risks – these disclosures appear to have happened *outside* of the Pentagon's network where traditional perimeter IT approaches and policies are not effective.
- One Source / Many Exposures – one source, in this case, adversely affected multiple government agencies. This exposure is worse than a lost laptop since P2P users have open access to the information on the computer without the knowledge of the owner. Anyone who knows what to look for can obtain this information and share it.
- Risk of "Open Windows" – whatever new files are now added to this individual's computer will then become available to the P2P user community. Despite the fact that sensitive files may or may not be

present on an employee or suppliers computer today, the very existence of P2P file sharing software can expose whatever files are added in the future.

Redacted examples that protect the privacy of the respective government agencies and affected individuals have been provided to the Committee with the exception of classified information which, as noted earlier, was provided to the Chairman of the National Intelligence Advisory Board by General Wesley Clark.

Law Enforcement Related Examples

Citizens expect our government to protect its own classified and confidential information, but to also enforce laws governing illegal uses and exploitation of information. Examples of this include enforcing copyright and licensing laws and export control laws. One example we wish to highlight to the committee is the extensive use of P2P Networks for searching and sharing child pornography. To illustrate the extent of this trafficking of this information, Tiversa collected searches that P2P users were issuing for known child pornography terms. This example is provided to the committee as a separate exhibit.

Live Demonstration

While the examples collected represent various periods of time, a glimpse into what is available *live* on P2P networks dramatically illustrates the extent of exposure for the categories of examples highlighted above. We will now show user issued searches and available files that match a select list of file probing terms.

Evidence of Wrong-doing

Tiversa has shown the committee live views of P2P user issued searches and available sensitive, inadvertently shared files. We have illustrated that P2P users are actively searching for sensitive, confidential, and classified information. We have shown sensitive, confidential, and classified files are present on P2P networks across individual consumer, corporate, and government sources. What happens to these files once they are found, downloaded, replicated, or used? Is there evidence of fraud or wrong doing?

Fraud Test

Tiversa, in conjunction with Dartmouth's Center for Digital Strategies, conducted a test to show that once a file with actionable financial information is inadvertently disclosed on a P2P network, individuals will use it for an ill-gotten financial gain.

Tiversa and Dartmouth purchased a VISA cash card and an AT&T calling card and incorporated the cash card numbers and phone card numbers instructions on how to use these into a letter. An electronic copy of the letter was put on a

Dartmouth test computer and shared using LimeWire file sharing software. Tiversa tracked the spread of the letter globally across P2P file sharing networks, from the point of initial compromise from the original source computer to its sharing and subsequent re-sharing(s). Tiversa and Dartmouth then tracked the real-time use of the cash card and calling card. The VISA cash card was depleted within a week. Even after the original source computer was shut off, the file continued to be shared by others users on P2P file sharing networks.

Professor Eric Johnson from Dartmouth will explain this test in more detail in later testimony to this committee.

Corporate Information Test

A similar Dartmouth experiment was conducted with documents related to a fictitious company placed on a Dartmouth test computer and shared using LimeWire file sharing software. Tiversa then tracked the spread of these files from the original source computer across P2P networks clearly indicating that there was significant "demand" for these "corporate" files.

The Root of the Problem

Why is there such a pervasive and massive amount of sensitive, classified, and confidential information available on peer-to-peer file sharing networks? Corporations and government agencies have installed technologies designed to block access to P2P networks and instituted policies that prohibit employees from using P2P networks or taking or e-mailing information to their homes. Consumers have installed virus checking and firewalls, which is typically the recommended course of action by the world's major security software providers.

Tiversa's focus has been working with corporations, government agencies, and consumers to mitigate P2P disclosures and risks. Based on our experience, we believe the reason so much information is present is driven by these factors:

1. A lack of awareness to the pervasiveness and magnitude of sensitive and classified information present on P2P networks. One cannot "fix" a problem that one is unaware of, no matter how much it currently may affect an organization.
2. Overextended information security functions and budgets that prioritize recent "fires" or compliance with legislation and industry mandates. Prioritizing something to which there is little awareness is often not done because it is difficult to gain the attention of senior management and procure budgets and resources.
3. Organizations have "too narrow" a view of their network perimeter. Whose responsibility is it to protect information once it leaves the corporate perimeter? Does a consumer or the US government care

whether a corporation or a supplier to that corporation entrusted with sensitive information disclosed files on P2P File Sharing Networks once the damage is done? The overwhelming evidence shows that a substantial amount of P2P inadvertent file sharing breaches come from an organization's *Extended Enterprise* outside of its network perimeter. Many organizations today focus solely on protecting their network perimeters when their business is becoming more virtual and outsourcing is taking hold. Sensitive, confidential, and classified information follows these new business operations.

Finding Solutions

We would like to provide the committee our initial recommendations on how consumers, corporations, and government entities can mitigate this problem.

The committee should take steps to:

- Create broader and more focused awareness of the dangers of inadvertent P2P file sharing.
- Require continuous auditing of P2P file sharing networks themselves for sensitive, confidential, and classified information disclosures.
- Encourage organizations to adopt policies and to take steps to address their *Extended Enterprise*.

Consumers:

For consumers, Tiversa has a number of recommended actions

- Consumers first need to become aware of this problem. While government warnings already exist, we feel the private sector can play a highly effective role in addressing this issue and in creating awareness. Banks, credit card companies, and healthcare insurance organizations can lead this effort since they are most impacted by P2P originated fraud. They are trusted by their customers and have existing communication channels available. Previous efforts to address phishing serve as a useful model.
- Consumers should consider putting their highly sensitive information on a separate PC or device disconnected from the Internet.
- Consumers should continuously audit P2P networks to ensure that unwanted files are not exposed. If they find personal or sensitive information available, they should be equipped with the knowledge of what actions to immediately take.

Corporate

For corporations, Tiversa has a number of recommended actions:

- Those tasked with managing security risks inside of an organization must be aware of the pervasiveness and magnitude of inadvertent P2P file sharing, and how it affects them. These individuals need to educate senior leadership – especially those in privacy, legal, and compliance – to the risks they face.
- Corporations need to understand their disclosed information exposure by auditing, as fully as possible by a neutral third party, the type and magnitude of their information on P2P file sharing networks.
- Corporations need to continuously monitor for new exposure points on P2P networks, and to judge the effectiveness of their policies and remedial actions.
- Corporations need to identify disclosure sources across their Extended Enterprises that expose them to inadvertent file sharing risks. This includes employees operating outside of the perimeter, suppliers and contractors, agents, and partners.
- Corporations should re-evaluate “four-wall” perimeter approaches to information security and update their policies to address information disclosure by third parties and the general lack of control once information exits an organization. This may include, for instance, requiring contractors, suppliers, attorneys, and accountants to indemnify the organization for peer-to-peer originated information disclosures.

Government

- The government should take the lead in creating greater awareness at corporations and throughout the public on the dangers associated with P2P file sharing.
- The government should immediately and continuously identify the full exposure and global spread of classified information to shut down these disclosure sources.
- The government should conduct a comprehensive audit of P2P file sharing network information disclosures – not just focused on the agencies themselves, but on also on contractors and non-agency sources.
- P2P information exposure risk should be emphasized in the Federal Information Security Management Act Report Card.

- The government should require their contractors to certify that they and their extended enterprises have fully addressed inadvertent file sharing disclosure risk.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, or classified information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of the technology in the future.

Thank you for the opportunity to testify here today.

Testimony Before the House Subcommittee on Commerce, Trade and Consumer Protection

Robert Boback, CEO, Tiversa, Inc.

May 4, 2009

TIERSA.

Good afternoon Chairman Rush, Ranking Member Radanovich and Distinguished Members of the Subcommittee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

As P2P file-sharing risk continues to be a major security, risk and privacy issue, let me first start by first providing a brief background on peer-to-peer.

It is important to note that the Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

Peer-to-peer networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

- 1 – Planned file sharing – its intended use.
- 2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

P2P networks continue to grow in size and popularity due to the alluring draw of the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie

and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may only want to share their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have adequately highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads a P2P software program on his/her parents computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software program variants that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program.

This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, and foreign intelligence worldwide.

Today, we would like to provide the committee with concrete examples that show the extent of the security problems that are present on the P2P networks and implications of sharing this type of information. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

Despite the tools that P2P network developers are putting into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the

dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

"By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers in previous hearings, the problem continues to exist. In fact, we will also seek to demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been architected in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previ-

ously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Financial Fraud

In an analysis of these searches, listed below is a small sampling of actual searches issued on P2P networks brief research window in March 2009. The term credit card was used as the filter criteria for the period.

2007 credit card numbers
2008 batch of credit cards
2008 credit card numbers
a&l credit card
aa credit card application
abbey credit cards
abbey national credit card
ad credit card authorization
april credit card information
athens mba credit card payment
atw 4m credit card application
austins credit card info
auth card credit
authorization credit card
authorization for credit card
authorize net credit card
bank and credit card informati
bank credit card
bank credit card information
bank credits cards passwords
bank numbers on credit cards
bank of america credit cards
bank of scotland credit card
bank staffs credit cards only
barnabys credit card personal
bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their

tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases where accountant and tax offices, themselves, are inadvertently disclosing client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately \$35. This is up from approximately \$8-\$10 only a few short years ago. One plausible explanation for rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSN. This is a very important point. Our search data shows that thieves in fact a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her tax return, it will automatically be rejected by the IRS's system as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims only to have the initial victim left to address the problem with the IRS. This is very costly and time consuming to resolve.

Stolen SSNs are also used by illegal aliens as a requirement of their gaining employment here in the United States. This crime has far reaching implications as well as a tremendous tax burden on behalf of the victim.

Medical Fraud

Medical information is also being sought after on P2P networks with alarming regularity. Listed below are some terms issued over the same period regarding medical information.

letter for medical bills
letter for medical bills dr
letter for medical bills etmc
letter re medical bills 10th
ltr client medical report
ltr hjh rosimah medical
ltr medical body4life
ltr medical maternity portland
ltr medical misc portland
ltr orange medical head center
ltr to valley medical
lytec medical billing
medical investigation
medical journals password
medical .txt

medical abuse records
medical abuse
medical abuse records
medical algorithms
medical authorization
medical authorization form
medical authorization
medical benefits
medical benefits plan chart
medical billing
medical billing
medical bill
medical biller resume
medical billing software
medical billing
medical billing windows

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, he or she would then immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which he or she would quickly turn into cash by selling the drugs. This is a very difficult crime to detect as most consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company which only serves to prolong the activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

Searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. In the full year of 2006 and 2007, the average annual rise in the search totaled just over 10%.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings in this testimony would put these corporations at further risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information.

The only correlation that we identified is that the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Child Predation

As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can become even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program.

Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

Examples to follow on subsequent pages...

Tiversa engaged in research involving over 30,000 consumers and found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the last 60 days (2/25-4/26), Tiversa has downloaded 3,908,060 files that have been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. Its important to note that these files were only downloaded with general industry terms and client filters running. Much more exists on the network in a given period of time.

This risk also extends to the military and to overall national security. Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of in excess of 200,000 of our troops.

This issue poses a national security risk. In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the Wall Street Journal printed a front cover story that indicated that former Pentagon officials had indicated that spies had downloaded plans for the \$300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Recommendations

Tiversa's focus has been working for several years with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and

protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

Awareness should extend to corporations as well. With consumers being asked to provide PII to employers, banks, accountants, doctors, hospitals, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary state to state and, in our experience, are seldom respected or followed by organizations.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. The breach law will also need to be enforced as many of the disclosing companies disregard the current state laws, if any to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel Disclosures

Congress should vigorously act to protect the safety and identity of our men and women in uniform. Soldiers who have had their information disclosed should be provided comprehensive identity theft protection services so as to prevent and guard against the use of the breached information.

National Security Disclosures

P2P networks should be continuously monitored globally for the presence of any classified or confidential information that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it)

Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask!

Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service

Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The subcommittee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify here today.



TIVERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940-9030 *office*
(724) 940-9033 *fax*
www.tiversa.com

Data Hemorrhages in the Health-Care Sector¹

M. Eric Johnson

Center for Digital Strategies
Tuck School of Business
Dartmouth College, Hanover NH 03755
M.Eric.Johnson@dartmouth.edu

Abstract. Confidential data hemorrhaging from health-care providers pose financial risks to firms and medical risks to patients. We examine the consequences of data hemorrhages including privacy violations, medical fraud, financial identity theft, and medical identity theft. We also examine the types and sources of data hemorrhages, focusing on inadvertent disclosures. Through an analysis of leaked files, we examine data hemorrhages stemming from inadvertent disclosures on internet-based file sharing networks. We characterize the security risk for a group of health-care organizations using a direct analysis of leaked files. These files contained highly sensitive medical and personal information that could be maliciously exploited by criminals seeking to commit medical and financial identity theft. We also present evidence of the threat by examining user-issued searches. Our analysis demonstrates both the substantial threat and vulnerability for the health-care sector and the unique complexity exhibited by the US health-care system.

Keywords: Health-care information, identity theft, data leaks, security.

1 Introduction

Data breaches and inadvertent disclosures of customer information have plagued sectors from banking to retail. In many of these cases, lost customer information translates directly into financial losses through fraud and identity theft. The health-care sector also suffers such data hemorrhages, with multiple consequences. In some cases, the losses have translated to privacy violations and embarrassment. In other cases, criminals exploit the information to commit fraud or medical identity theft.

¹ Experiments described in this paper were conducted in collaboration with Tiversa who has developed a patent-pending technology that, in real-time, monitors global P2P file sharing networks. The author gratefully acknowledges the assistance of Nicholas Willey. This research 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). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

Given the highly fragmented US health-care system, data hemorrhages come from many different sources—ambulatory health-care providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back-offices of health maintenance organizations, and outsourced service providers such as billing, collection, and transcription firms.

In this paper we analyze the threats and vulnerabilities to medical data. We first explore the consequences of data hemorrhages, including a look at how criminals exploit medical data, in particular through medical identity theft. Next, we examine types and sources of data hemorrhages through a direct analysis of inadvertent disclosures of medical information on publically available, internet-based file sharing networks. We present an analysis of thousands of files we uncovered. These files were inadvertently published in popular peer-to-peer file sharing networks like Limewire and Bearshare and could be easily downloaded by anyone searching for them. Originating from health-care firms, their suppliers, and patients themselves, the files span everything from sensitive patient correspondence to business documents, spreadsheets, and PowerPoint files. We found multiple files from major health-care firms that contained private employee and patient information for literally tens of thousands of individuals, including addresses, Social Security Numbers, birth dates, and treatment billing information. Disturbingly, we also found private patient information including medical diagnoses and psychiatric evaluations. Finally, we present evidence, from user-issued searches on these networks, that individuals are working to find medical data—likely for malicious exploitation.

The extended enterprises of health-care providers often include many technically unsophisticated partners who are more likely to leak information. As compared with earlier studies we conducted in the banking sector (Johnson 2008), we find that tracking and stopping medical data hemorrhages is more complex and possibly harder to control given the fragmented nature of the US health-care system. We document the risks and call for better control of sensitive health-care information.

2 Consequences of Data Hemorrhages

Data hemorrhages from the health-care sector are diverse, from leaked business information and employee personally identifiable information (PII) to patient protected health information (PHI), which is individually identifiable health information. While some hemorrhages are related to business information, like marketing plans or financial documents, we focus on the more disturbing releases of individually identifiable information and protected health information. In these cases, the consequences range from privacy violations (including violations of both state privacy laws and federal HIPPA standards) to more serious fraud and theft (Figure 1).

On one hand, health-care data hemorrhages fuel financial identity theft. This occurs when leaked patient or employee information is used to commit traditional financial fraud. For example, using social security numbers and other identity information to apply for fraudulent loans, take-over bank accounts, or charge purchases to credit cards. On the other hand, PHI is often used by criminals to commit traditional medical fraud, which typically involves billing payers (e.g.,

Medicaid/Medicare or private health-care insurance) for treatment never rendered. The US General Accounting Office estimated that 10% of health expenditure reimbursed by Medicare is paid to fraudsters, including identity thieves and fraudulent health service providers (Bolin and Clark 2004; Lafferty 2007).

PHI can also be very valuable to criminals who are intent on committing medical identity theft. The crime of medical identity theft represents the intersection of medical fraud and identity theft (Figure 1). Like medical fraud, it involves fraudulent charges and like financial identity theft, it involves the theft of identity. It is unique in that it involves a medical identity (patient identification, insurance information, medical histories, prescriptions, test results...) that may be used to obtain medical services or prescription drugs (Ball et al. 2003). Leaked insurance information can be used to fraudulently obtain service, but unlike a credit card the spending limits are much higher—charges can quickly reach tens of thousands or even millions of dollars. And unlike financial credit, there is less monitoring and reporting. Sadly, beyond the financial losses, medical identity theft carries other personal consequences for victims as it often results in erroneous changes to medical records that are difficult and time consuming to correct. Such erroneous information could impact care quality or impede later efforts to obtain medical, life, or disability insurance.

For example, recent medical identity theft cases have involved the sale of health identities to illegal immigrants (Messmer 2008). These forms of theft are a problem impacting payers, patients, and health-care providers. Payers and providers both see financial losses from fraudulent billing. Patients are also harmed when they are billed for services they did not receive, and when erroneous information appears on their medical record.

Between 1998 and 2006, the FTC recorded complaints of over nineteen thousand cases of medical identity theft with rapid growth in the past five years. Many believe these complaints represent the tip of the growing fraud problem, with some estimates showing upwards of a quarter-million cases a year (Dixon 2006, 12-13). Currently, there is no single agency tasked with tracking, investigating, or prosecuting these crimes (Lafferty 2007) so reliable data on the extent of the problem does not exist.

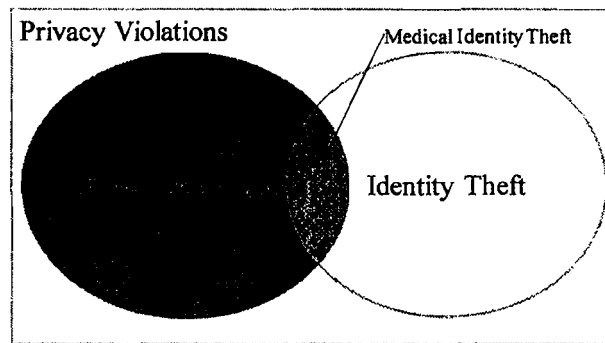


Fig. 1. Consequences of data hemorrhages.

The crime of financial identity theft is well understood with clear underlying motives. A recent FTC survey estimated that 3.7% of Americans were victims of some sort of identity theft (FTC 2007). Significant media coverage has alerted the public of the financial dangers that can arise when a thief assumes your identity. However, the dangers and associated costs of medical identity theft are less well understood and largely overlooked. Of course, PHI (including insurance policy information and government identity numbers) can be fraudulently used for financial gain at the expense of firms and individuals. However, when a medical identity is stolen and used to obtain care, it may also result in life-threatening amendments to a medical file. Any consequential inaccuracies in simple entries, such as allergy diagnoses and blood-typing results, can jeopardize patient lives. Furthermore, like financial identity theft, medical identity theft represents a growing financial burden on the private and public sectors.

Individuals from several different groups participate in the crime of medical identity theft: the uninsured, hospital employees, organized crime rings, illegal aliens, wanted criminals, and drug abusers. In many cases the theft is driven by greed, but in other case the underlying motive is simply for the uninsured to receive medical care. Without medical insurance, these individuals are unable to obtain the expensive care that they require, such as complicated surgeries or organ transplants. However, if they assume the identity of a well insured individual, hospitals will provide full-service care. For example, Carol Ann Hutchins of Pennsylvania assumed another woman's identity after finding a lost wallet (Wereschagin 2006). With the insurance identification card inside the wallet, Hutchins was able to obtain care and medication on 40 separate occasions at medical facilities across Pennsylvania and Ohio, accumulating a total bill of \$16,000. Had it not been for the victim's careful examination of her monthly billing statement, it is likely that Hutchins would have continued to fraudulently receive care undetected. Hutchins served a 3-month jail sentence for her crime, but because of privacy laws and practices, any resulting damage done to the victim's medical record was difficult and costly to erase.

Hospital employees historically comprise the largest known group of individuals involved in traditional medical fraud. They may alter patient records, use patient data to open credit card accounts, overcharge for and falsify services rendered, create phony patients, and more. The crimes committed by hospital employees are often the largest, most intricate, and the most costly.

Take for example the case of Cleveland Clinic front desk clerk coordinator, Isis Machado who sold the medical information of more than 1,100 patients, to her cousin Fernando Ferrer, Jr., the owner of Advanced Medical Claims Inc. of Florida. Fernando then provided the information to others who used the stolen identities to file an estimated \$7.1 million in fraudulent claims (USDC 2006).

Individuals abusing prescription drugs also have a motive to commit medical identity theft. Prescription drug addicts can use stolen identities to receive multiple prescriptions at different pharmacies. Drugs obtained through this method may also be resold or traded. Roger Ly, a Nevada pharmacist allegedly filed and filled 55 false prescriptions for Oxycontin and Hydrocodone in the name of customers. Medicare and insurance paid for the drugs that Ly, allegedly, then resold or used recreationally (USA 2007). The total value of drugs sold in the underground prescription market

likely exceeds \$1 billion (Peterson 2000). Sometimes, the crimes involving prescription drugs are less serious; a Philadelphia man stole a coworker's insurance identification card to acquire a Viagra prescription, which he filled on 38 separate occasions. The plan finally backfired when the coworker he was posing as attempted to fill his own Viagra prescription and discovered that one had already been filled at another pharmacy. The cost to his company's insurance plan: over \$3,000 (PA 2006).

Wanted criminals also have a strong motive to commit medical identity theft. If they check into a hospital under their own name, they might be quickly apprehended by law enforcement. Therefore, career criminals need to design schemes to obtain care. Joe Henslik, a wanted bank robber working as an ad salesman, found it easy to obtain Joe Ryan's Social Security number as part of a routine business transaction (BW 2007). Henslik then went on to receive \$41,888 worth of medical care and surgery under Ryan's name. It took Ryan two years to discover that he had been a victim of medical identity theft. Even after discovery, he found it difficult to gain access to his medical records, since his own signature didn't match that of Henslik's forgery.

Anndorie Sachs experienced a similar situation when her medical identity was used to give birth to a drug addicted baby (Reavy 2006). Sachs had lost her purse prior to the incident and had accordingly cancelled her stolen credit cards, but was unaware of the risk of medical ID theft. The baby, which was abandoned at the hospital by the mother, tested positive for illegal drug use, prompting child services to contact Sachs, who had four children of her own. Fortunately, since Sachs did not match the description of the woman who gave birth at the hospital, the problem did not escalate further. If Sachs was not able to prove her identity, she could have lost custody of her children, and been charged with child abuse. Furthermore, before the hospital became aware of the crime, the baby was issued a Social Security number in Sachs name, which could cause complications for the child later in life. Like Sachs, few individuals consider their insurance cards to be as valuable as the other items they carry in their wallet. Moreover, medical transactions appearing on a bill may not be scrutinized as closely as financial transactions with a bank or credit card.

Illegal immigrants also represent a block of individuals with a clear motive to commit medical identity theft. In the case of a severe medical emergency, they will not be refused care in most instances, but if an illegal immigrant requires expensive surgery, costly prescriptions, or other non-emergency care, they have few options. One of the most shocking and well documented cases comes from Southern California, where a Mexican resident fooled the state insurance program, Medi-Cal, into believing that he was a resident and therefore entitled to health care coverage (Hanson 1994). Mr. Hermillo Meave, was transferred to California from a Tijuana, Mexico hospital with heart problems, but told the California hospital that he was from San Diego, and provided the hospital with a Medi-Cal ID card and number. Although the circumstances surrounding Mr. Meave's arrival were suspicious, the hospital went ahead and completed a heart transplant on Mr. Meave. The total cost of the operation was an astounding one million dollars. Only after the surgery did the hospital determine that Mr. Meave actually lived and worked in Tijuana and was therefore not entitled to Medi-Cal coverage.

Perhaps emboldened by the success of Hermillo Meave, a family from Mexico sought a heart transplant for a dying relative just three months later at the very same

hospital. This time, fraud investigators were able to discover the plot before the surgery could be completed. While processing the paperwork for the patient who was checked in as Rene Garcia, Medi-Cal authorities found nine other individuals around the state, using the same name and ID number. The hospital had the family arrested and jailed for the attempted fraud, which had cost the hospital \$200,000, despite the lack of surgery. The family told investigators that they had paid \$75,000 in order to obtain the ID and set up the surgery. The trafficking of identities between Mexico and California is commonplace, but the sale of Medi-Cal identities adds a new dimension to the crime. The disparity in care between California hospitals and Mexican facilities makes the motivation to commit medical identity theft clear: falsified identification is a low-cost ticket to world-class care.

Finally, identity theft criminals often operate in crime rings, sometimes using elaborate ruses to gather the identities of hundreds of individuals. In a Houston case, criminals allegedly staged parties in needy areas offering medical deals as well as food and entertainment (USDJ 2007). At the parties, Medicaid numbers of residents were obtained and then used to bill Medicaid for alcohol and substance abuse counseling. The scheme even included fraudulent reports, written by 'certified' counselors. The fraudulent company managed to bill Medicaid for \$3.5M worth of services, of which they received \$1.8M. In this case, no medical care was actually administered and the medical identity theft was committed purely for financial reasons.

In summary, there are many reasons why individuals engage in medical identity theft, including avoiding law enforcement, obtaining care that they have no way of affording, or simply making themselves rich. Many tactics are used including first hand by physical theft, insiders, and harvesting leaked data. As we saw, PHI can be sold and resold before theft occurs—as in the case of the nine Garcias. The thief may be someone an individual knows well or it could be someone who they've never met.

For health-care providers, the first step in reducing such crime is better protection of PHI by: 1) controlling access within the enterprise to PHI; 2) securing networks and computers from direct intruders; 3) monitoring networks (internal and external) for PII and PHI transmissions and disclosures; 4) avoiding inadvertent disclosures of information. Often loose access and inadvertent disclosures are linked. When access policies allow many individuals to view, move, and store data in portable documents and spreadsheets, the risk of inadvertent disclosure increases.

3 Inadvertent Data Hemorrhages

Despite the much trumpeted enactment of the Health Insurance Portability and Accountability Act (HIPAA), data losses in the health-care sector continue at a dizzying pace. While the original legislation dates back to 1996, the privacy rules regulating the use and disclosure of medical records did not become effective until 2004. Moreover, the related security rules, which mandate computer and building safeguards to secure records, became effective in 2005. While firms and organizations have invested to protect their systems against direct intrusions and hackers, many recent the data hemorrhages have come from inadvertent sources. For

example, laptops at diverse health organizations including Kaiser Permanente (Bosworth 2006), Memorial Hospital (South Bend IN) (Tokars 2008), the U.S. Department of Veterans Administration (Levitz and Hechinger 2006), and National Institutes of Health (Nakashima and Weiss 2008) were lost or stolen—in each case inadvertently disclosing personal and business information.

Organizations have mistakenly posted on the web many different types of sensitive information, from legal to medical to financial. For example, Wuesthoff Medical Center in Florida inadvertently posted names, Social Security numbers and personal medical information of more than 500 patients (WFTV 2008). Insurance and health-care information of 71,000 Georgia residents was accidentally posted on Internet for several days by Tampa-based WellCare Health Plans (Hendrick 2008).

The University of Pittsburgh Medical Center inadvertently posted patient information of nearly 80 individuals including names and medical images. In one case, a patient's radiology image was posted along with his Social Security number, insurance information, medications, and with information on previous medical screenings and procedures (Twedt, 2007). Harvard University and its pharmacy partner, PharmaCare (now part of CVS Caremark), experienced a similar embarrassment when students showed they could easily gain access to lists of prescription drugs bought by Harvard students (Russell 2005). Even technology firms like Google and AOL have suffered the embarrassment of inadvertent web posting of sensitive information (Claburn 2007, Olson 2006)—in their cases, customer information. Still other firms have seen their internal information and intellectual property appear on music file-sharing networks (DeAvila 2007), blogs, YouTube, and MySpace (Totty 2007). In each case, the result was the same: sensitive information inadvertently leaked creating embarrassment, vulnerabilities, and financial losses for the firm, its investors, and customers. In a recent data loss, Pfizer faces a class action suit from angry employees who had their personal information inadvertently disclosed on a popular music network (Vijayan 2007). In this paper we examine health-care leaks from a common, but widely misunderstood source of inadvertent disclosure: peer-to-peer file-sharing networks.

In our past research, we showed that peer-to-peer (P2P) file-sharing networks represented a significant security risk to firms operating within the banking sector (Johnson and Dynes, 2007; Johnson 2008). File sharing became popular during the late 1990s with rise of Napster. In just two years before its court-ordered closure in 2001, Napster enabled tens of millions of users to share MP3-formatted song files. Through its demise, it opened the door for many new P2P file-sharing networks such as Gnutella, FastTrack, e-donkey, and Bittorrent, with related software clients such as Limewire, KaZaA, Morpheus, eMule, and BearShare. Today P2P traffic levels are still growing with as many as ten million simultaneous users (Mennecke 2006). P2P clients allow users to place shared files in a particular folder that is open for other users to search. However, there are many ways that other confidential files become exposed to the network (see Johnson et al. 2008 for a detailed discussion). For example a user: 1) accidentally shares folders containing the information—in some cases confusing client interface designs can facilitate such accidents (Good and Krekelberg (2003)); 2) stores music and other data in the same folder that is shared—this can happen by mistake or because of poor file organization; 3) downloads

malware that, when executed, exposes files; or 4) installs sharing client software that has bugs, resulting in unintentional sharing of file directories.

While these networks are most popularly used to trade copyrighted material, such as music and video, any material can be exposed and searched for including databases, spreadsheets, Microsoft Word documents, and other common corporate file formats. The original exposure of this material over P2P networks is most likely done by accident rather than maliciously, but the impact of a single exposure can quickly balloon. After a sensitive file has been exposed, it can be copied many times by virtually anonymous P2P users, as they copy the file from one another and expose the file to more peers. Criminals are known to engage in the sale and trafficking of valuable information and data. In earlier studies using "honeypot" experiments (experiments that expose data for the purpose of observing how it is stolen), we showed how criminals steal and use both consumer data and corporate information (Johnson et al. 2008). When this leaked information happens to be private customer information, organizations are faced with costly and painful consequences resulting from fraud, customer notification, and consumer backlash.

Ironically, individuals who experience identity theft often never realize how their data was stolen. While there are many ways personal health-care data can be exposed, we will show in the next section how data hemorrhages in P2P networks represent a missing link in the "causality chain." Far worse than losing a laptop or a storage device with patient data (Robenstein 2008), inadvertent disclosures on P2P networks allow many criminals access to the information, each with different levels of sophistication and ability to exploit the information. And unlike an inadvertent web posting, the disclosures are far less likely to be noticed and corrected (since few organizations monitor P2P and the networks are constantly changing making a file intermittently available to a subset of users). Clearly, such hemorrhages violate the privacy and security rules of HIPAA, which call for health-care organizations to ensure implementation of administrative safeguards (in the form of technical safeguards and policies, personnel and physical safeguards) to monitor and control intra and inter-organizational information access.

4 Research Method and Analysis

To explore the vulnerability and threat of medical information leakage, we examined health-care data disclosures and search activity in peer-to-peer file sharing networks. To collect a sample of leaked data, we initially focused on Fortune Magazine's list of the top ten publically traded health-care firms (Fortune Magazine (Useem 2007)). Together those firms represented nearly \$70B in US health-care spending (Figure 2).

To gather relevant files, we developed a digital footprint for each health-care institution. A digital footprint represents key terms that are related to the firm—for example names of the affiliated hospitals, clinics, key brands, etc. Searching the internet with Google or P2P networks using those terms will often find files related to those institutions. With the help of Tiversa Inc., we searched P2P networks using our digital signature over a 2-week period (in January, 2008) and randomly gathered a sample of shared files related to health care and these institutions. Tiversa's servers

and software allowed us 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). Files containing any one or combination of these terms in our digital footprint were captured. We focused on files from the Microsoft Office Suite (Word, Powerpoint, Excel, and Access). Of course, increasing the number of terms included in the digital footprint increases the number file matches found, but also increases false positives—files captured that have nothing to do with the institution in question. Given the large number of hospitals within these ten organizations (more than 500), our goal was to gather a sample of files to characterize the ongoing data hemorrhage. Since users randomly join P2P networks to get and share media (and then depart), the network is constantly changing. By randomly sampling over a 14-day period, we collected 3,328 files for further (manual) analysis.

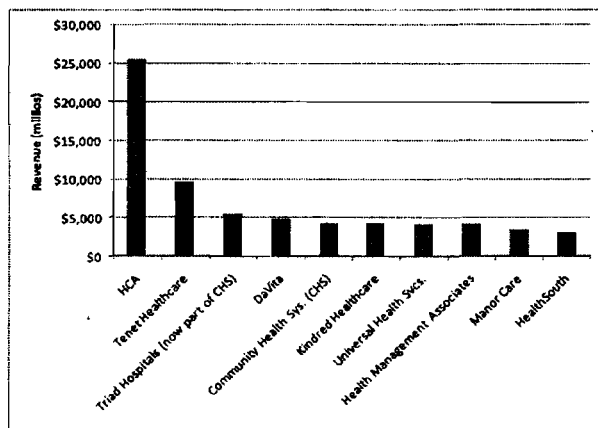


Fig. 2. Revenue of the top ten US health-care firms (Useem 2007).

Of 3,328 documents in our sample, 50.3% could be immediately identified as duplicate copies of the same file (same hash) that had spread or were on multiple IP addresses, leaving us with 1,654 documents to categorize. While duplicate files were not downloaded from the same IP address, duplicate files were collected when a target file had spread to multiple sharing clients. They were also collected from users who joined the network at different IP addresses (what we call an IP shift). Through a manual analysis of the remaining 1,654 files, we found that 71% were not relevant to health care or the organizations under consideration and were downloaded because our search terms overlapped with other subject matter. This was the result of the size and quality of our digital footprint. By casting a large net, we found more files but also many that were not related to the health-care sector. Of the remaining 475 documents, 86 were manually evaluated as duplicate files. With this cross section of

data associated with the health-care organizations, we categorized each file evaluating the dangers associated with it. Figure 3 shows a categorization of the 389 unique, relevant files.

The most common type of files found were newspaper and journal articles, followed by documents associated with students studying medicine. This should not come as a surprise as many P2P users are students. Interestingly, we found entire medical texts being shared. We also found many documents dealing directly with medical issues, such as billings, letters to hospitals, and insurance claims. Many of these documents were leaked by patients themselves. For example, we found several patient-generated spreadsheets containing details of medical treatments and costs—likely for tax purposes. Other documents discovered included hospital brochures and flyers, which were intended for public consumption. Finally there were job listings, cover letters, and résumés, all likely saved on computers of job-seekers. The lack interest in sharing these files for a typical P2P user makes it readily apparent that they were likely shared by mistake. However, all of the files weren't so innocuous. After categorizing the files, we found that about 5% of the files recovered by our loosely tuned search were sensitive or could be used to commit medical or financial identity theft.

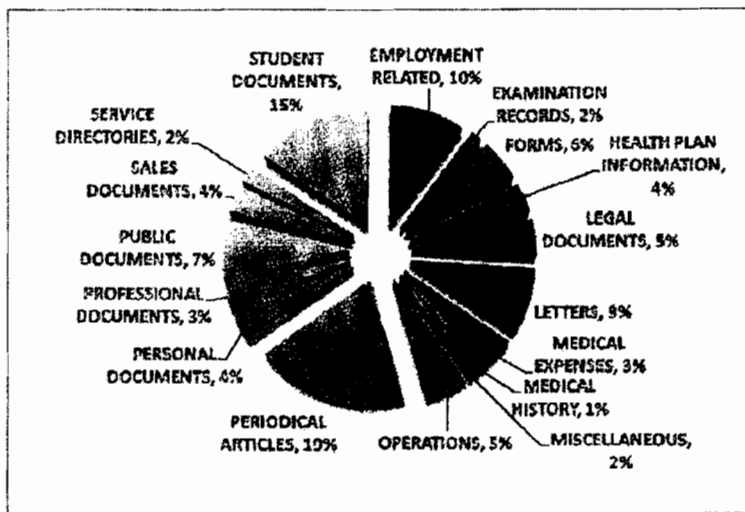


Fig. 3. Summary of unique relevant files.

The set of dangerous documents discovered contained several files that would facilitate medical identity theft. One such document was a government application for employment asking for detailed background information. The document contained the individual's Social Security number, full name, date of birth, place of

birth, mother's maiden name, history of residence and acquaintances, schooling history, and employment history (the individual had worked at one of the hospitals under study). Despite the document's three-page forward highlighting the privacy act measures undertaken by the government to protect the information in the document, and the secure Data Hash code stamped at the bottom of every page along with the bolded text 'PRIVACY ACT INFORMATION', this document somehow ended up on to a P2P network.

More disturbing, we found a hospital-generated spreadsheet of personally identifiable information on recently-hired employees including Social Security numbers, contact information, job category etc. Another particularly sensitive document was an Acrobat form used for creating patient prescriptions. The scanned blank document was signed by a physician and allowed for anyone to fill in the patient's name and prescription information. This document could be used for medical fraud by prescription drug dealers and abusers. Additionally, the doctor's own personal information was included in the document, giving criminals the opportunity to forge other documents in his name. Finally, another example we found was a young individual's medical card. This person was suffering from various ailments and was required to keep a card detailing his prescription information. The card included his doctor's name, parent's names, address, and other personal information. A person with a copy of this identification card could potentially pose as the patient and attempt to procure prescription drugs. All of these dangerous files were found with a relatively simple sample of files published for anyone to find.

As a second stage of our analysis, we then moved from sampling with a large net to more specific and intentional searches. Using information from the first sampling, we examined shared files on hosts where we had found other dangerous data. One of the features enabled by Limewire and other sharing clients is the ability to examine all the shared files of a particular user (sometimes called "browse host"). Over the next six months, we periodically examined hosts that appeared promising for shared files.

Using this approach, we uncovered far more disturbing files. For a medical testing laboratory, we found a 1,718-page document containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients. Figure 4 shows a redacted excerpt of just a single page of the insurance aging report containing patient name, Social Security number, date of birth, insurer, group number, and identification number. All together, almost 9,000 patient identities were exposed in a single file, easily downloaded from a P2P network.

| Insurance Aging | | | | | | | | | |
|---|---------------|------------|------------|-------|----------|--------|--------|--------|----------|
| [REDACTED] INCORPORATED | | | | | | | | | |
| [REDACTED] | | | | | | | | | |
| Date of Birth: [REDACTED] Insured: Self | | | | | | | | | |
| Insurance: Primary | ID: | | | | | | | | |
| [REDACTED] | 05/01/2008 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | 12/17/2008 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | 04/03/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | 231.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 228.00 | 231.00 |
| Insurance Total: | | 377.18 | 0.00 | 0.00 | 0.00 | 147.78 | 231.46 | 378.16 | |
| Date of Birth: [REDACTED] Insured: Self | | | | | | | | | |
| Insurance: Primary | Group Number: | ID: | | | | | | | |
| [REDACTED] | [REDACTED] | 02/17/2008 | 08/29/2008 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 |
| [REDACTED] | [REDACTED] | 08/10/2008 | 08/10/2008 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | [REDACTED] | 12/09/2008 | 12/09/2008 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | | | 41.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| Insurance Total: | | | | 82.00 | 0.00 | 0.00 | 0.00 | 82.00 | 82.00 |
| Date of Birth: [REDACTED] Insured: Self | | | | | | | | | |
| Insurance: Primary | Group Number: | ID: | | | | | | | |
| [REDACTED] | [REDACTED] | 05/19/2008 | 05/19/2008 | 41.00 | 0.00 | 0.00 | 0.00 | 0.00 | 41.00 |
| Patient Total: | | | | 41.00 | 0.00 | 0.00 | 0.00 | 41.00 | 41.00 |
| Insurance Total: | | | | 82.00 | 0.00 | 0.00 | 0.00 | 82.00 | 82.00 |
| Date of Birth: [REDACTED] Insured: Self | | | | | | | | | |
| Insurance: Secondary | ID: | | | | | | | | |
| [REDACTED] | 03/02/2007 | 05/04/2007 | 110.00 | 0.00 | 0.00 | 110.00 | 0.00 | 0.00 | 110.00 |
| [REDACTED] | 09/05/2007 | 05/04/2007 | -18.00 | 0.00 | 0.00 | -18.00 | 0.00 | 0.00 | -18.00 |
| [REDACTED] | 03/02/2007 | 05/04/2007 | 110.00 | 0.00 | 0.00 | 110.00 | 0.00 | 0.00 | 110.00 |
| [REDACTED] | 09/11/2007 | 05/24/2007 | 3300.00 | 0.00 | 3300.00 | 0.00 | 0.00 | 0.00 | 3300.00 |
| [REDACTED] | 09/17/2007 | 05/24/2007 | -2128.40 | 0.00 | -2128.40 | 0.00 | 0.00 | 0.00 | -2128.40 |
| [REDACTED] | 05/17/2007 | 05/24/2007 | -624.00 | 0.00 | -624.00 | 0.00 | 0.00 | 0.00 | -624.00 |
| Patient Total: | | | 459.60 | 0.00 | 227.60 | 818.00 | 0.00 | 0.00 | 459.60 |
| Date of Birth: [REDACTED] Insured: Self | | | | | | | | | |
| Insurance: Primary | ID: | | | | | | | | |
| [REDACTED] | 01/23/2007 | 02/02/2007 | 25.70 | 0.00 | 0.00 | 0.00 | 0.00 | 25.70 | 25.70 |
| [REDACTED] | 02/23/2007 | 02/23/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| [REDACTED] | 04/24/2007 | 04/24/2007 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Patient Total: | | | 25.70 | 0.00 | 0.00 | 0.00 | 0.00 | 25.70 | 25.70 |
| Insurance Total: | | | 25.70 | 0.00 | 0.00 | 0.00 | 0.00 | 25.70 | 25.70 |

Fig. 4. Excerpt of an insurance aging report. It contains 1718 pages of patient names, social security numbers, and dates of birth, insurers, group numbers, and identification numbers (exposing nearly 9000 patients). Personally Identifiable Information has been redacted to protect the identities of the disclosers and patients.

For a hospital system, we found two spreadsheet databases that contained detailed information on over 20,000 patients including Social Security numbers, contact details, and insurance information. Up to 82 fields of information (see Figure 5) were recorded for each patient—representing the contents of the popular HCFA form. In this case, the hemorrhage came from an outsourced collection agency working for the hospital. However, besides the patients and hospital system, many other

| | | |
|---------------------------------|-----------------------------------|---------------------------------|
| 1. FAFA billNumber | 28. dischargeDate | 55. firstInsuranceName |
| 2. providerName | 29. patientMedRecNo | 56. firstInsuranceAddressLine1 |
| 3. providerAddressLine1 | 30. patientMaritalStatus | 57. firstInsuranceCity |
| 4. providerCityStateZip | 31. guarantorFirstName | 58. firstInsuranceState |
| 5. providerPhoneNumber | 32. guarantorLastName | 59. firstInsuranceZipCode |
| 6. providerFederalTaxId | 33. guarantorSSN | 60. firstPolicyNumber |
| 7. patientFirstName | 34. guarantorPhone | 61. firstAuthorizationNumber |
| 8. patientMiddleInitial | 35. guarantorAddressLine1 | 62. firstGroupName |
| 9. patientLastName | 36. guarantorAddressLine2 | 63. firstGroupNumber |
| 10. patientSSN | 37. guarantorCity | 64. firstInsuredRelationship |
| 11. patientPhone | 38. guarantorState | 65. firstDateEligible |
| 12. patientAddressLine1 | 39. guarantorZipCode | 66. firstDateThru |
| 13. patientAddressLine2 | 40. guarantorBirthDate | 67. secondInsuranceName |
| 14. patientCity | 41. guarantorEmployerName | 68. secondInsuranceAddressLine1 |
| 15. patientState | 42. guarantorEmployerAddressLine1 | 69. secondInsuranceCity |
| 16. patientZipCode | 43. guarantorEmployerAddressLine2 | 70. secondInsuranceState |
| 17. patientSex | 44. guarantorEmployerCity | 71. secondInsuranceZipCode |
| 18. patientBirthDate | 45. guarantorEmployerState | 72. secondPolicyNumber |
| 19. patientEmployerName | 46. guarantorEmployerZipCode | 73. secondGroupName |
| 20. patientEmployerAddressLine1 | 47. guarantorEmployerPhone | 74. secondGroupNumber |
| 21. patientEmployerAddressLine2 | 48. guarantorRelationship | 75. secondInsuredRelationship |
| 22. patientEmployerCity | 49. totalCharges | 76. secondDateEligible |
| 23. patientEmployerState | 50. amountBalance | 77. secondDateThru |
| 24. patientEmployerZipCode | 51. totalPayments | 78. primaryDiagnosisCode |
| 25. patientEmployerPhone | 52. totalAdjustments | 79. attendingPhysician |
| 26. caseType | 53. accidentCode | 80. attendingPhysicianUPIN |
| 27. admissionDate | 54. accidentDate | 81. lastPaymentDate |
| | | 82. providerShortName |

Fig. 5. File contents for over 20,000 patients in on inadvertent disclosure.

organizations were comprised. The data disclosed in this file well-illustrates the complexity of US health care with many different constituencies represented, including 4 major hospitals, 335 different insurance carriers acting on behalf of 4,029 patient employers, and 266 different treating doctors (Figure 6). Each of these constituents was exposed in this disclosure. Of course, the exposure of sensitive patient health-information may be the most alarming to citizens. Figure 7 shows one very small section of the spreadsheet (just three columns of 82) for a few patients (of the nearly 20,000). Note that the diagnosis code (IDC code) is included for each patient. For example, code 34 is streptococcal sore throat; 42 is AIDS; 151.9 is malignant neoplasm of stomach (cancer); 29 is alcohol-induced mental disorders; and 340 is multiple sclerosis. In total the file contained records on 201 patients with different forms of mental illness, 326 with cancers, 4 with AIDS, and thousands with other serious and less serious diagnoses.

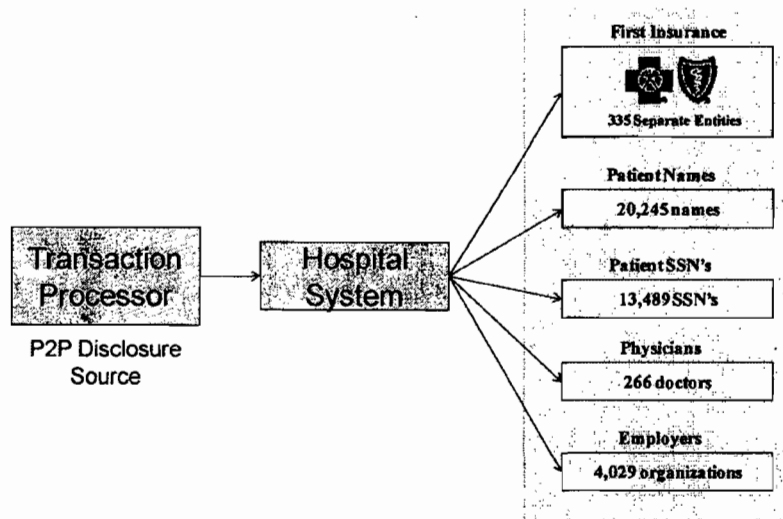


Fig. 6. Hemorrhage exposed a large array of health-care constituents.

| CA | CB | CC |
|----------------------|--------------------|-----------------------|
| primaryDiagnosisCode | attendingPhysician | attendingPhysicianUPN |
| 8.45 | | |
| 34 | | |
| 34 | | |
| 34 | | |
| 42 | | |
| 151.9 | | |
| 152.1 | | |
| 291 | | |
| 291.81 | | |
| 292 | | |
| 292.82 | | |
| 340 | | |
| 340 | | |
| 780.39 | | |
| 780.39 | | |
| 780.4 | | |
| 780.6 | | |
| 780.6 | | |
| 780.79 | | |
| 780.79 | | |
| 780.99 | | |
| 789 | | |
| 798 | | |
| 923 | | |
| V70.0 | | |
| V76.12 | | |
| V76.54 | | |

Fig. 7. Disclosures expose extremely personal diagnosis information. A very small section of a spreadsheet for a few (of over 20,000) patients showing IDC diagnosis codes (see <http://www.cms.hhs.gov/ICD9ProviderDiagnosticCodes/> or <http://www.icd9data.com/>). Personally Identifiable Information has not been included in the illustration to protect the identities of the patients and physicians.

For a mental health center, we found patient psychiatric evaluations. All would be considered extremely personal and some were disturbing. We found similar clinical evaluations leaking from Alabama to Nebraska to California.

Of course, these are just few of many files we uncovered. For a group of anesthesiologists, we found over 350MB of data comprising patient billing reports. For a drug and alcohol rehab center, we found similar billing information. From an AIDs clinic we found a spreadsheet with 232 clients including address, Social Security number, and date of birth. And the list goes on. It is important to note that all of these files were found without extraordinary effort and certainly far less effort than criminals might be economically incented to undertake.

With the vulnerability well established, we also investigated the search activity in P2P networks to see if users were looking for health-care data hemorrhages. Again, using our simple digital signature we captured a sample of user-issued searches along with our files. Figure 8 lists a sample of these searches and clearly shows that users are searching for very specific health-care related data in P2P networks.

| | | | |
|--------------------------------|-------------------------------|-------------------------------|--------------------------------|
| care office nbc health | billy connolly medical | dear medical assurance my | letter for medical bills |
| medicine mental health cro of | checkup | dear medical insurance my | letter for medical bills dr |
| hospital records | billy connolly medical check | dear medical my assurance | letter for medical bills etmc |
| mental hospitals | canada medical test | denial of medical insurance | letter re medical bills 10th |
| hospital | canadian medical | denial medical cross coding | ltr client medical report |
| hospital letterhead | canadian medical association | detective medical | ltr hgh rosimah medical |
| hospital records | canadian medical law | digital files medical trans | ltr medical body4life |
| niagara hospital | caulfield general medical | distributeur medical | ltr medical maternity portland |
| american medical | cbib clic1 medical expenses | doctor - medical checkup | ltr medical misc portland |
| connolly medical ups prostate | certificat medical | doctor fake medical by exam | ltr orange medical head center |
| data entry medical billing fax | certificat medical | doctor medical exam | ltr to valley medical |
| dear medical insurance my | certifica medical | Doctors medical billing | lytec medical billing |
| denial of medical insurance | certificat medical | doctors office medical exam | medical investigation |
| hendee w r medical imaging | charfee medical costs | doctors order medical doctor | medical journals password |
| isilo medical | charfee medical costs on the | doctors orders medical | medical.txt |
| medical | child medical exam | doug medical bill | medical abuse records |
| medical claims | child medical exams | doug stanhope medical pms | medical abuse |
| medical exam | child medical release form | edimis medical software 3.9 | medical abuse records |
| medical history | cigna medical dr | electronic medical | medical algorithms |
| medical passwords | cigna medical drs | electronic medical record | medical authorization |
| medical permission | classified medical records | electronic medical record osx | medical authorization form |
| medical records certification | complete medical exam | electronic medical record.pdf | medical authorization |
| medical release | comprehensive medical | electronic medical records | medical benefits |
| medical secretary cover letter | computoc medical | electronic medical systems | medical benefits plan chart |
| medicine medical passwords | computerize medical | electronics & bio medical | medical billing |
| authorization for medical | computerize medical billing | emt medical software | medical billing |
| authorization for medical of c | tu | forms medical | medical bill |
| authorization for medical of j | computers in the medical offi | forms medical liability form | medical biller resume |
| authorization form medical | computers medical doctors | forme medical office | medical billing software |
| basic medical forms | connelly medical check billy | ge medical | medical billing |
| basic medical laboratory techn | connelly medical ups | ge medical systems | medical billing windows |
| benny medical jack insurance | billing medical august | medical coding and billing | |
| billing medical | | medical coding exam | |

Fig. 8. Selection of User-Issued searches that contain the word medical or hospital

5 Conclusion

Data hemorrhages from the health-care sector are clearly a significant threat to providers, payers, and patients. The inadvertent disclosures we found and documented in this report point to the larger problem facing the industry. Clearly, such hemorrhages may fuel many types of crime. While medical fraud has long been a significant problem, the crime of medical identity theft is still in its infancy. Today, many of the well-documented crimes appear to be committed out of medical need. However, with the growing opportunity to commit more significant crimes involving large financial rewards, more and more advanced schemes and methods, such as P2P-fueled identity theft, will likely develop. For criminals to profit, they don't need to "steal" an identity, but only to borrow it for a few days, while they bill the insurer carrier thousands of dollars for fabricated medical bills. This combination of medical fraud along with identity theft adds a valuable page to the playbook of thieves looking for easy targets. Stopping the supply of digital identities is one key to halting this type of illegal activity.

The Health Insurance Privacy Accountability Act (HIPAA) was created to protect patients from having sensitive medical information from becoming public or used against them. However, some of the provisions of the act make medical identity theft more difficult to track, identify, and correct. Under HIPAA, when a patient's medical record has been altered by someone else using their ID, the process to correct the record is difficult for the patient. The erroneous information in the medical file may remain for years. Also due to the intricacies of HIPAA, people who have been victims of medical identity theft may find it difficult to even know what has been changed or added to their record. Since the thief's medical information is contained within the victim's file, it is given the same privacy protections as anyone under the act. Without the ability to remove erroneous information, or figure out the changes contained in a medical record, repairing the damages of medical identity theft can be a very taxing process.

However, HIPAA is also a positive force in the fight against identity theft. Institutions have been fined and required to implement detailed corrective action plans to address inadvertent disclosures of identifiable electronic patient information (HHS 2008). In the case of Isis Machado mentioned earlier, she was charged and fined under HIPAA for disclosing individually identifiable medical records. HIPAA contains rules and punishments for offending medical professionals, which are historically the largest group of health-care fraud perpetrators. This protection of patient identities does discourage inappropriate uses of medical information and reduces the chance of hemorrhages. Nevertheless, HIPAA can do little to stop patients from disclosing their medical identities voluntarily to individuals posing as health care providers, or poorly managing their own computerized documents.

Tighter controls on patient information are a good start, but consumers still need to be educated of the dangers of lost health-care information and how to secure their information on personal computers. Hospitals and others concerned with medical identity theft have begun to undertake measures in order to curb medical identity theft. One of the simplest and most effective measures put in place by hospitals is to request photo identification for admittance to the hospital. In many cases, when a request for photo identification is made, the individual will give up on obtaining care and simply leave the hospital, never to return again. Of course, this measure will likely lose its efficacy in time as criminals become aware of the change in policy. Once a few personal identifiers have been acquired, such as date of birth and Social Security number, a criminal can obtain seemingly valid photo-ID. In the future, insurance companies may need to begin issuing their own tamper-proof photo identification to help stop medical identity theft.

Finally, health-care providers and insurers must enact better monitoring and information controls to detect and stop leaks. Information access within many health-care systems is lax. Coupled with the portability of data, inadvertent disclosures are inevitable. Better control over information access governance (Zhao and Johnson 2008) is an important step in reducing the hemorrhages documented in this report.

References

1. Ball, E., Chadwick, D.W., Mundy, D (2003), "Patient Privacy in Electronic Prescription Transfer," *IEEE Security & Privacy*, March/ April, 77 – 80.
2. Bolin, J.N., Clark, L.S. (2004), "Avoiding Charges of Fraud and Abuse: Developing and Implementing an Effective Compliance Program," *JONA* (34:12), 546-550.
3. Bosworth, M.H. (2006), "Kaiser Permanente Laptop Stolen: Personal Data on 38,000 Members Missing," *Consumer Affairs*, Nov 29, http://www.consumeraffairs.com/news04/2006/11/kaiser_laptop.html
4. BW (2007), "Diagnosis: Identity Theft," *Business Week*, January 8, 2007.
5. Claburn, T. (2007), "Minor Google Security Lapse Obscures Ongoing Online Data Risk," *Information Week*, January 22.
6. De Avila, J. (2007), "The Hidden Risk of File-Sharing," *Wall Street Journal*, Nov. 7, D1.
7. Dixon, P. (2006), "Medical Identity Theft: The Information Crime that Can Kill You," *The World Privacy Forum*.
8. FBI (2007), "2006 Financial Crime Report" Federal Bureau of Investigation. [Online] 02 28, 2007. [Cited: 02 04, 2008.] http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm.
9. FTC (2007), "2006 Identity Theft Report," Federal Trade Commission, November, 2007, last accessed on June 18, 2008, <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>
10. Good N.S., and A. Krekelberg (2003) "Usability and privacy: a study of Kazaa P2P file-sharing," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, April 05-10.
11. Hanson, G (1994), "Illegal Aliens Bilk Sick U.S. system," *Insight on the News*. April 18, 1994.
12. Hendrick, B. (2008), "Insurance records of 71,000 Ga. families made public," *Atlanta Journal-Constitution*, April 08. http://www.ajc.com/metro/content/metro/stories/2008/04/08/breach_0409.html
13. HHS (2008), "HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information," U.S. Department of Health & Human Services, News Release, July 17, <http://www.hhs.gov/news/press/2008pres/07/20080717a.html>
14. Johnson, M. E. and S. Dynes (2007), "Inadvertent Disclosure: Information Leaks in the Extended Enterprise," *Proceedings of the Sixth Workshop on the Economics of Information Security*, Carnegie Mellon University, June 7-8.
15. Johnson, M. E. (2008), "Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain," *Journal of Management Information Systems*, Vol. 25, No. 2, 97-123.
16. Johnson, M. E., D. McGuire, and N. D. Willey (2008), "The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users," *Proceedings of HICSS-41, International Conference on System Sciences*, IEEE Computer Society, Jan 7-10, Hawaii.
17. Johnson, M. E., McGuire, D., and N. D. Willey (2009), "Why File Sharing Networks Are Dangerous," *Communications of the ACM*, 52, 2, 134-138.
18. Lafferty, L (2007), "Medical Identity Theft: The Future Threat of Health Care Fraud Is Now," *Journal of Health Care Compliance*; Jan/Feb, 9, 1, 11-20.
19. Levitz, J. and J. Hechinger (2006), "Laptops Prove Weakest Link in Data Security," *Wall Street Journal*, March 26.
20. Mennecke, T. (2006), "Slyck News - P2P Population Continues Climb," June 14, <http://www.slyck.com/news.php?story=1220>

21. Messmer, E. (2008), "Health Care Organizations See Cyberattacks as Growing Threat," *Network World*, February 28.
22. Musco, T. D. and K. H. Fyffe (1999), "Health Insurers' Anti-fraud Programs," Washington D.C. Health Insurance Association of America.
23. Nakashima, E. and R. Weiss (2008), "Patients' Data on Stolen Laptop," *Washington Post*, March 24, A1.
24. Olson, P. (2006), "AOL Shoots Itself in the Foot," *Forbes*, August 8.
25. PA (2006), "Pennsylvania Attorney General. Attorney General's Insurance Fraud Section charges former SEPTA employee with using co-worker's ID to obtain Viagra." Harrisburg: s.n., July 6, 2006.
26. Peterson, M. (2000), "When Good Drugs Go Gray; Booming Underground Market Raises Safety Concerns," *The New York Times*, 12 14, 2000, p. 1.
27. Reavy, P. (2006), "What Baby? ID victim gets a jolt," *Deseret News* (Salt Lake City). May 2, 2006.
28. Robenstein, S. (2008), "Are Your Medical Records at Risk?" *Wall Street Journal*,
29. Russell, J. (2005), "Harvard fixing data security breaches: Loophole allowed viewing student prescription orders" *Boston Globe*, January 22.
30. Tokars, L. (2008), "Memorial Hospital loses laptop containing sensitive employee data," *WSBT*, Feb 7, <http://www.wsbt.com/news/local/15408791.html>
31. Totty, M. (2007), "Security: How to Protect Your Private Information," *Wall Street Journal*, January 29. R1.
32. Twedt, S. (2007), "UPMC patients' personal data left on Web," *Pittsburgh Post-Gazette*, April 12.
33. USDC (2006), "United States of America vs. Fernando Ferrer, Jr. and Isis Machado," 06-60261, s.l., United States District Court Southern District of Florida, September 7, 2006.
34. USDJ (2007), "US Department of Justice. Six Indicted for Health Care Fraud Scheme in Southeast Texas," Houston, TX: s.n., 2007. Press Release.
35. USA (2007), "United States Attorney, District of Nevada. "Las Vegas Pharmacist Charged with Health Care Fraud and Unlawful Distribution of Controlled Substances," Las Vegas, United States Department of Justice, 2 23, 2007.
36. Useem, J. (2007), "Fortune 500: The Big Get Bigger," *Fortune Magazine*, 155, 8, April 30, 81. *Wall Street Journal*, March 26.
37. Vijayan, J. (2007), "Personal data on 17,000 Pfizer employees exposed; P2P app blamed," *Computer World*.
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024491>
38. Wereschagin, Mike (2006), "Medical ID Theft Leads to Lengthy Recovery." *Pittsburgh Tribune-Review*, 10 24, 2006.
39. WFTV (2008), "Medical Center Patient Records Posted On Internet," August 14, <http://www.wftv.com/news/17188045/detail.html?taf=orc>
40. Zhao, X. and M. E. Johnson (2008), "Information Governance: Flexibility and Control through Escalation and Incentives," *Proceedings of the Seventh Workshop on the Economics of Information Security*, Dartmouth College, June 26-27.

Testimony Before the House Subcommittee on Commerce, Trade and Consumer Protection

Robert Boback, CEO, Tiversa, Inc.

May 4, 2009

TIVERSA.

Good afternoon Chairman Rush, Ranking Member Radanovich and Distinguished Members of the Subcommittee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

As P2P file-sharing risk continues to be a major security, risk and privacy issue, let me first start by first providing a brief background on peer-to-peer.

It is important to note that the Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

Peer-to-peer networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

- 1 – Planned file sharing – its intended use.
- 2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

P2P networks continue to grow in size and popularity due to the alluring draw of the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie

and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may only want to share their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have adequately highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads a P2P software program on his/her parents computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software program variants that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program.

This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, and foreign intelligence worldwide.

Today, we would like to provide the committee with concrete examples that show the extent of the security problems that are present on the P2P networks and implications of sharing this type of information. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

Despite the tools that P2P network developers are putting into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the

dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

"By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers in previous hearings, the problem continues to exist. In fact, we will also seek to demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been architected in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previ-

ously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, approximately 8 times that of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Financial Fraud

In an analysis of these searches, listed below is a small sampling of actual searches issued on P2P networks brief research window in March 2009. The term credit card was used as the filter criteria for the period.

2007 credit card numbers
2008 batch of credit cards
2008 credit card numbers
ach credit card
aa credit card application
abbey credit cards
abbey national credit card
ad credit card authorization
april credit card information
athens mba credit card payment
atw 4m credit card application
austins credit card info
auth card credit
authorization credit card
authorization for credit card
authorize net credit card
bank and credit card informati
bank credit card
bank credit card information
bank credits cards passwords
bank numbers on credit cards
bank of america credit cards
bank of scotland credit card
bank staffs credit cards only
barnabys credit card personal
bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their

tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases where accountant and tax offices, themselves, are inadvertently disclosing client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately \$35. This is up from approximately \$8-\$10 only a few short years ago. One plausible explanation for rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSN. This is a very important point. Our search data shows that thieves in fact a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her tax return, it will automatically be rejected by the IRS's system as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims only to have the initial victim left to address the problem with the IRS. This is very costly and time consuming to resolve.

Stolen SSNs are also used by illegal aliens as a requirement of their gaining employment here in the United States. This crime has far reaching implications as well as a tremendous tax burden on behalf of the victim.

Medical Fraud

Medical information is also being sought after on P2P networks with alarming regularity. Listed below are some terms issued over the same period regarding medical information.

letter for medical bills
letter for medical bills dr
letter for medical bills etmc
letter re medical bills 10th
ltr client medical report
ltr hjh rosimah medical
ltr medical body4life
ltr medical maternity portland
ltr medical misc portland
ltr orange medical head center
ltr to valley medical
lytec medical billing
medical investigation
medical journals password
medical .txt

medical abuse records
medical abuse
medical abuse records
medical algorithms
medical authorization
medical authorization form
medical authorization
medical benefits
medical benefits plan chart
medical billing
medical billing
medical bill
medical biller resume
medical billing software
medical billing
medical billing windows

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, he or she would then immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which he or she would quickly turn into cash by selling the drugs. This is a very difficult crime to detect as most consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company which only serves to prolong the activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

Searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. In the full year of 2006 and 2007, the average annual rise in the search totaled just over 10%.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings in this testimony would put these corporations at further risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information.

The only correlation that we identified is that the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Child Predation

As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can become even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program.

Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

Examples to follow on subsequent pages...

| 4 | A | B | C | D | E | F | G | H | I | J | K | L |
|------|----------|-------------|---|---|---|---|-------------|-------|--------|------------|-------|--------|
| 9501 | HOSPITAL | JANIELA | | | | | HOUSTON | 77053 | Female | 12/4/1978 | | 222.71 |
| 9502 | HOSPITAL | MARQUE | | | | | BRIDGE CITY | 77611 | Female | 02/21/1973 | | 183 |
| 9503 | HOSPITAL | PAULEA | | | | | BRIDGE CITY | 77611 | Female | 10/24/1964 | | 768.4 |
| 9504 | HOSPITAL | MARTINE | | | | | BRIDGE CITY | 77611 | Male | 4/18/1962 | | 173.42 |
| 9505 | HOSPITAL | LUKES | | | | | HOUSTON | 77052 | Male | 02/19/1978 | | 316.8 |
| 9506 | HOSPITAL | MILLIAM | | | | | DALLAS | 75226 | Male | 11/7/1952 | NON D | 316.8 |
| 9507 | HOSPITAL | ANDREA | | | | | PORT ARTHUR | 77662 | Female | 10/30/1980 | | 278.83 |
| 9508 | HOSPITAL | BRENDA | | | | | UDCA | 77628 | Male | 02/21/1977 | | 780.3 |
| 9509 | HOSPITAL | ESPERANZA | | | | | TOLAND PARK | 75382 | Female | 12/24/1963 | | 785.33 |
| 9510 | HOSPITAL | RYAN | | | | | DALLAS | 75226 | Male | 5/18/1978 | | 180 |
| 9511 | HOSPITAL | IMANES | | | | | PORT NECHER | 77651 | Male | 10/29/1977 | NON D | 180 |
| 9512 | HOSPITAL | LOHREY | | | | | HOUSTON | 77052 | Male | 1/28/1982 | | 431.73 |
| 9513 | HOSPITAL | LOHREY | | | | | DALLAS | 75211 | Male | 12/31/1963 | | 716.57 |
| 9514 | HOSPITAL | DAVE | | | | | BRIDGE CITY | 77611 | Male | 11/11/1958 | | 611.74 |
| 9515 | HOSPITAL | STEPHEN | | | | | ORANGE | 77668 | Male | 11/28/1962 | | 8.3 |
| 9516 | HOSPITAL | CARLOS | | | | | DALLAS | 75226 | Female | 1/28/1969 | | 789.3 |
| 9517 | HOSPITAL | CHRISTOPHER | | | | | PT ARTHUR | 77662 | Male | 10/27/1978 | | 323.3 |
| 9518 | HOSPITAL | DAVID | | | | | HOUSTON | 77052 | Male | 10/21/1964 | | 758.3 |
| 9519 | HOSPITAL | SHANA | | | | | ORANGE | 77668 | Female | 8/9/1978 | | 218.41 |
| 9520 | HOSPITAL | MICHAEL | | | | | HOUSTON | 77052 | Male | 1/10/1978 | | 232.51 |
| 9521 | HOSPITAL | ROBERTO | | | | | BRIDGE CITY | 77611 | Male | 12/17/1962 | | 216.71 |
| 9522 | HOSPITAL | YOLANDA | | | | | DALLAS | 75226 | Female | 1/24/1970 | NON D | 216.71 |
| 9523 | HOSPITAL | LEI | | | | | DALLAS | 75226 | Male | 3/17/1971 | | 411.83 |
| 9524 | HOSPITAL | ROSE | | | | | DALLAS | 75226 | Female | 10/26/1964 | | 922.3 |
| 9525 | HOSPITAL | EVLYA | | | | | HOUSTON | 77052 | Female | 2/4/1960 | | 710.3 |
| 9526 | HOSPITAL | CHRISTOPHER | | | | | HOUSTON | 77052 | Male | 1/9/1968 | | 821 |
| 9527 | HOSPITAL | ELVENA | | | | | PORT ARTHUR | 77662 | Female | 10/19/1969 | | 717.83 |
| 9528 | HOSPITAL | BERRY | | | | | HOUSTON | 77052 | Male | 7/27/1967 | | 278.43 |
| 9529 | HOSPITAL | MICHAEL | | | | | DALLAS | 75226 | Female | 1/28/1962 | | 278.43 |
| 9530 | HOSPITAL | LEI | | | | | PORT ARTHUR | 77662 | Male | 1/14/1962 | | 782.3 |
| 9531 | HOSPITAL | LEI | | | | | PORT ARTHUR | 77662 | Female | 10/17/1963 | | 368 |
| 9532 | HOSPITAL | A | | | | | ORANGE | 77668 | Male | 3/8/1966 | | 428 |
| 9533 | HOSPITAL | CATER | | | | | PORT ARTHUR | 77662 | Male | 1/10/1960 | | 217.83 |
| 9534 | HOSPITAL | JOSE | | | | | DALLAS | 75211 | Male | 11/17/1967 | | 812.3 |
| 9535 | HOSPITAL | MARY | | | | | DALLAS | 75211 | Female | 12/24/1977 | | 164.3 |
| 9536 | HOSPITAL | MARY | | | | | DALLAS | 75211 | Male | 02/19/1962 | | 716.3 |
| 9537 | HOSPITAL | MARY | | | | | DALLAS | 75211 | Male | 11/23/1978 | | 560 |
| 9538 | HOSPITAL | PATRICIA | | | | | PORT ARTHUR | 77662 | Female | 11/4/1962 | | 396.3 |
| 9539 | HOSPITAL | MEREDITH | | | | | HOUSTON | 77052 | Female | 02/28/1963 | | 411.78 |
| 9540 | HOSPITAL | BERNADINE | | | | | HOUSTON | 77052 | Male | 3/24/1962 | | 221.23 |
| 9541 | HOSPITAL | BERNADINE | | | | | DALLAS | 75211 | Female | 3/14/1968 | | 364 |
| 9542 | HOSPITAL | EMERALDA | | | | | PORT ARTHUR | 77662 | Female | 3/17/1965 | | 717.83 |
| 9543 | HOSPITAL | ALEJANDRA | | | | | HOUSTON | 77052 | Female | 1/27/1969 | | 718.3 |
| 9544 | HOSPITAL | JOHN | | | | | BRIDGE CITY | 77662 | Male | 3/11/1962 | | 635.3 |
| 9545 | HOSPITAL | CAROLAN | | | | | HOUSTON | 77052 | Male | 02/21/1979 | | 272.53 |
| 9546 | HOSPITAL | JOYCE | | | | | DALLAS | 75211 | Female | 1/17/1933 | | 522.4 |

| 4 | Last | First | SSN | Taxable? | Degree | School | Major | Division |
|------|-------------|-------|-----|----------|-------------|----------------------------|-------------------|-----------|
| 1000 | John | | | N | Certificate | CFA Institute | CFA | Eastern |
| 1001 | Zishan | | | N | Graduate | NYIT | MBA | Western |
| 1002 | David | | | N | Certificate | CFA Institute | CFA | Western |
| 1003 | Anthony | | | N | Graduate | Stevens Institute | MIS | Eastern |
| 1004 | Measas | | | N | Certificate | Dowling College | CFP | Eastern |
| 1005 | Thomas | | | N | Certificate | Pace | CFP | Eastern |
| 1006 | Mary Linley | | | N | Certificate | American College | CFP | Eastern |
| 1007 | Samuel | | | N | Certificate | Kaplan University | CFP | Eastern |
| 1008 | Sandeep | | | N | Graduate | Steven Institute | Info Mgmt sys | Eastern |
| 1009 | Emmee | | | N | Certificate | Kaplan | CFP | SouthWest |
| 1010 | Scott | | | N | Certificate | Kaplan | CFP | Western |
| 1011 | Darya | | | N | Undergrad | Montclair State University | Marketing | Eastern |
| 1012 | Isaac | | | N | Certificate | Pace University | CFP | Eastern |
| 1013 | Sotland | | | N | Certificate | Kaplan | CFP | Eastern |
| 1014 | James | | | N | Certificate | Kaplan | CFP | Eastern |
| 1015 | Steven | | | N | Graduate | University of Connecticut | MBA | Eastern |
| 1016 | Michael | | | N | Graduate | Stevens Ins | MIS | Eastern |
| 1017 | Alejandra | | | N | Degree | Pace University | BA | Eastern |
| 1018 | Hasan | | | N | Undergrad | NYU | International MBA | Eastern |
| 1019 | Sneh | | | N | Undergrad | Stevens Institute | MIS | Eastern |
| 1020 | Luis | | | N | Undergrad | Aca College | BA | Eastern |
| 1021 | Jared | | | N | Certificate | Kaplan | CFP | Eastern |
| 1022 | Matthew | | | N | Undergrad | Brooklyn College | Finance | Eastern |
| 1023 | Francisco | | | N | Certificate | CFA Institute | CFA | Eastern |
| 1024 | Belinda | | | N | Undergrad | Universidad | Accounting | PR |

Tiversa engaged in research involving over 30,000 consumers and found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the last 60 days (2/25-4/26), Tiversa has downloaded 3,908,060 files that have been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. Its important to note that these files were only downloaded with general industry terms and client filters running. Much more exists on the network in a given period of time.

This risk also extends to the military and to overall national security. Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of in excess of 200,000 of our troops.

This issue poses a national security risk. In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the Wall Street Journal printed a front cover story that indicated that former Pentagon officials had indicated that spies had downloaded plans for the \$300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Recommendations

Tiversa's focus has been working for several years with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and

protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

Awareness should extend to corporations as well. With consumers being asked to provide PII to employers, banks, accountants, doctors, hospitals, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary state to state and, in our experience, are seldom respected or followed by organizations.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. The breach law will also need to be enforced as many of the disclosing companies disregard the current state laws, if any to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel Disclosures

Congress should vigorously act to protect the safety and identity of our men and women in uniform. Soldiers who have had their information disclosed should be provided comprehensive identity theft protection services so as to prevent and guard against the use of the breached information.

National Security Disclosures

P2P networks should be continuously monitored globally for the presence of any classified or confidential information that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it)

Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask!

Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service

Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The subcommittee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify here today.



TIVERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940-9030 *office*
(724) 940-9033 *fax*
www.tiversa.com

Testimony before the House Committee on Oversight and Government Reform

Robert Boback, CEO, Tiversa, Inc.

July 29, 2009

TI ERSA.

EXHIBIT - D

Good morning Chairman Towns, Ranking Member Issa and Distinguished Members of the Committee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

P2P file-sharing continues to be a major security risk and privacy issue. Today, I will provide a brief background on P2P networks, highlight the risks of inadvertent file sharing, provide examples of P2P file disclosures and the impact on consumers, businesses, government, the military and national security, and share our observations and recommendations.

Background: Peer-to-Peer Networks

The Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

P2P networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The P2P networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

P2P networks are growing and dynamic. Since 2005, P2P networks have grown at the rate of over 20% (CAGR). Today, worldwide P2P networks may have over 20 million users at any point in time. P2P networks are ever-changing as users join and exit constantly. The number of P2P programs or "clients" has grown to over 225, with many having multiple versions in use. Additionally, many of the

programs are open source and, accordingly, subject to modification as users see fit. P2P networks are a worldwide phenomenon with users across wide ranges of ages, educational backgrounds and incomes.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

- 1 – Planned file sharing – its intended use.
- 2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
- 3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

Inadvertent File Disclosure

P2P networks continue to grow in size and popularity due to the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this unintentional sharing that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may want to share only their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads P2P software program on his/her parents' computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software programs that Tiverse has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program. This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs typically do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial

infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, foreign intelligence organizations and terrorists worldwide.

Despite the tools that P2P network developers are incorporating into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as data loss prevention, firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

"By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

Today, we will provide the Committee with concrete examples that show the extent of the security problems that exist on the P2P networks and the implications of sharing this type of information. During our testimony, we will provide the Committee with examples that illustrate the types of sensitive information available on P2P networks, provide examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers and government agencies in previous hearings, the problem remains. In fact, we will also demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Tiversa and Its Technology

Beginning in 2003, Tiversa developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been designed, developed and implemented in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, more than the number of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Tiversa uses this technology to provide P2P security and intelligence services to businesses, consumers and law enforcement agencies. The following examples demonstrate how inadvertent breaches affect individual consumers, businesses, government, military and national security and are based on our unique perspective on P2P networks.

Examples: Inadvertent Disclosures on P2P

Consumers

Financial Fraud – From analysis of P2P searches, listed below is a small sampling of actual searches issued on P2P networks during a brief research window in March 2009. The term *credit card* was used as the filter criteria for the period.

- 2007 credit card numbers
- 2008 batch of credit cards
- 2008 credit card numbers
- a&l credit card
- aa credit card application
- abbey credit cards
- abbey national credit card
- ad credit card authorization
- april credit card information
- athena mba credit card payment
- atw 4m credit card application
- austins credit card info
- auth card credit
- authorization credit card
- authorization for credit card
- authorize net credit card
- bank and credit card informati
- bank credit card
- bank credit card information
- bank credits cards passwords
- bank numbers on credit cards
- bank of america credit cards
- bank of scotland credit card
- bank staffs credit cards only
- barnabys credit card personal
- bibby chase credit card

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January of this year for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases in which accountants and tax offices, themselves, inadvertently disclosed client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately \$35 each. This is up from approximately \$8-\$10 only a few short years ago. One plausible explanation for the rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSNs. This is a very important point. Our search data shows that thieves in fact employ a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her legitimate tax return, it will automatically be rejected by the IRS as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims leaving the initial victim to address the problem with the IRS. This is very costly and time consuming for both the victim and the IRS.

Stolen SSNs are also used by illegal aliens to gain employment in the United States. This crime has far reaching implications as well as placing a tremendous tax burden on the victim.

Medical Fraud – Medical information is also being targeted on P2P networks with alarming and increasing regularity. Listed below are some terms issued over the same period regarding medical information.

- *letter for medical bills*
- *letter for medical bills dr*
- *letter for medical bills etmc*
- *letter re medical bills 10th*
- *ltr client medical report*
- *ltr hjh rosimah medical*
- *ltr medical body4life*
- *ltr medical maternity portland*
- *ltr medical misc portland*
- *ltr orange medical head center*
- *ltr to valley medical*
- *lytec medical billing*
- *medical investigation*
- *medical journals password medical .txt*
- *medical abuse records*
- *medical abuse*
- *medical abuse records*
- *medical algoritms*

- *medical authorization*
- *medical authorization form*
- *medical authorization*
- *medical benefits*
- *medical benefits plan chart*
- *medical billing*
- *medical billing*
- *medical bill*
- *medical biller resume*
- *medical billing software*
- *medical billing*
- *medical billing windows*

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, the thief would immediately have access to significant financial resources (in many cases medical insurance policies have limits set at \$1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which can be quickly sold for cash. This is a very difficult crime to detect as many consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company, prolonging the criminal activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for valid medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

User-issued P2P searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. For the years of 2006 and 2007, the average annual rise in the search totaled just over 10%.

Child Predation – As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can be even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos

and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program and have been seeking to work more extensively with other law enforcement and prosecutorial organizations.

Tiversa has used its ability to locate available files and track individual's P2P network searches to document cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Sources of the Breach – Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

In research involving over 30,000 consumers, Tiversa found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the 60 day research period (2/25-4/26/09), Tiversa downloaded 3,908,060 files that had been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. It is important to note that these files were only downloaded with general industry terms and client filters running. Many more exist on the network in a given period of time.

Corporations and businesses

As a matter of record, Tiversa observes searches

similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of specific search strings in this testimony would put these corporations at further risk. General search terms include company names in combination with "confidential," "executive," "payroll" and other terms clearly designed to identify files containing important or personal information. The Committee should note that the searches of this nature are every bit as aggressive and more specific than those for credit cards and medical information – the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Corporate information disclosed on P2P networks includes breached PII and personal health information (the basis for much of the personal information used in identity theft described above), intellectual property, strategic documents and business plans. We have identified disclosures of legal documents, performance reviews, Board minutes, merger and acquisition plans, plant physical security plans, network diagrams, user ID's and passwords. Specific examples of inadvertent disclosures are described below.

One Supplier affects Thousands – In one instance, we identified one small company with fewer than 12 employees that provides third party billing services to hospitals. An inadvertent disclosure on patients from three different hospitals by this company exposed personal health information (patient names, SSNs, diagnosis codes, physician names, and other information) involving:

- 20,245 Patients
- 268 Physicians
- 4,029 Employer Organizations
- 335 Insurance Providers

It is easy to see the criminal value of the information exposed in this single breach and the potential impact to a broad range of individuals, professionals and organizations.

Corporate secrets revealed – In another instance, Tiversa discovered the PST file of a high-ranking officer involved in the merger and acquisition area of a Fortune 100 company. The entire Microsoft Outlook information of this officer was exposed to the public:

- Entire calendar
- Schedule of conference calls with dial-in numbers and passcodes
- Business and personal contacts including names, e-mails, addresses, phone numbers, etc.
- Over 12,000 e-mails to and from the individual
- Over 400 e-mail attachments (documents, PowerPoints, spreadsheets, etc.) Including:
 - Regional sales information
 - M&A business integration updates
 - Strategic business alliances
 - Revenues through acquisitions

In the wrong hands, this information could be used for individual profit from trading on "insider information" not formally reported by the company, or on a much larger scale to manipulate and undermine the credibility of the capital markets.

Government, the Military and National Security

This risk also extends to the military and to overall national security.

Troop PII exposed – Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of more than 200,000 of our troops.

Classified information searched for...and found – P2P networks also pose a national security risk. In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Searches are directed at identifying and obtaining sensitive information on matters of security using terms such as:

- Classified
- Military classified
- Military confidential
- Top secret
- US Marines classified
- Restricted

Examples of information breaches emanating from P2P networks and known to the public are described below.

In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the *Wall Street Journal* printed a front cover story reporting that former Pentagon officials had indicated that spies had downloaded plans for the \$300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter

program was also discovered on P2P networks.

Recommendations

For several years, Tiversa's focus has been working with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

FTC – On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

SEC – Awareness should extend to corporations and government agencies as well. Corporations regularly breach personal information of individuals (employees, customers, etc.). With consumers increasingly being asked to provide PII to employers, banks, accountants, doctors, hospitals, and government agencies, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Corporations also disclose non-public information that could be used for individual profit or to manipulate or undermine the markets. P2P risks and vulnerabilities that lead to these disclosures should be addressed in the application of current laws (Sarbanes-Oxley, Gramm-Leach-Bliley, etc.).

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary from state to state and, in our experience, are seldom respected or followed by organizations. In some cases, companies that seek to do the right thing are unfamiliar with the various laws that may apply to their situation or have difficulty in complying with the applicable laws.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. In this regard, we believe that P2P risks and vulnerabilities should be addressed in the application of current laws, and we support HR 2221 – the Data Accountability and Trust Act. This proposed legislation requires the establishment and implementation of policies and procedures for information security practices and includes notification and remediation provisions in instances of breach.

The breach laws will also need to be enforced. Many disclosing companies disregard the current state laws, if any, to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel & National Security Disclosures

DOD – The safety and identity of our men and women in uniform of Congress should be vigorously protected. Measures should be taken to safeguard personal information, and to monitor, detect and remediate any disclosures. For soldiers who have had their information disclosed, comprehensive identity theft protection services should be provided to prevent and guard against the use of the breached information.

DSS – P2P networks should be continuously monitored globally for the presence of any classified or confidential information disclosed by defense contractors or subcontractors that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it) – Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask! Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service – Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The Committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify today.

TI ERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

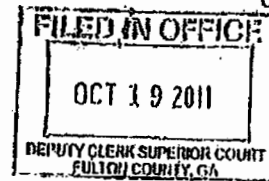
(724) 940-9030 office
(724) 940-9033 fax
www.tlvera.com



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

1.

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,

2

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 hererin.

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 Defendants' position as Director of the McNamee 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

LimeWire. 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 275,000 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 PII and/or PHI, 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.¹

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.

¹ 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 HE 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 File 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 44th 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:

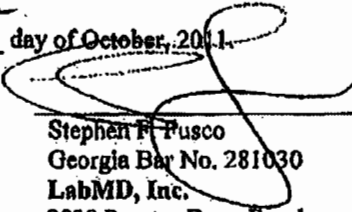
- (a) Judgment against Defendants as outlined herein;
- (b) Damages in an amount to be determined at trial;
- (c) Exemplary damages in an amount to be determined at trial.
- (d) Attorney's fees and costs associated with this litigation;
- (e) A trial by jury on the issues outlined herein;
- (f) All such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

proper.

Page

[SIGNATURE CONTINUE ON NEXT PAGE]

Respectfully submitted this 7 day of October, 2011.



Stephen F. 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.

FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL DAUGHERTY

PETITION EXHIBIT 6

Commission Letter Denying LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand, in File No. 102 3099 (April 20, 2012)



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

April 20, 2012

VIA E-MAIL AND COURIER DELIVERY

Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP
2900 K Street, N.W.
North Tower - Suite 200
Washington, D.C. 20007
E-mail: claudia.callaway@kattenlaw.com

RE: *LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand; and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand*

Dear Ms. Callaway, Ms. Grigorian, and Mr. Dayal:

On January 10, 2012, the Federal Trade Commission ("FTC" or "Commission") received the above Petitions filed by LabMD, Inc. ("LabMD") and its President, Michael J. Daugherty (collectively, "Petitioners"). This letter advises you of the Commission's disposition of the Petitions, effected through this ruling by Commissioner Julie Brill, acting as the Commission's delegate.¹

For the reasons explained below, the Petitions are denied. You may request review of this ruling by the full Commission.² Any such request must be filed with the Secretary of the Commission within three days after service of this letter ruling.³ The timely filing

¹ See 16 C.F.R. § 2.7(d)(4).

² 16 C.F.R. § 2.7(f).

³ *Id.* This ruling is being delivered by e-mail and courier delivery. The e-mail copy is provided as a courtesy, and the deadline by which an appeal to the full Commission

of a request for review by the full Commission shall not stay the return dates established by this ruling.⁴

I. INTRODUCTION

The FTC commenced its investigation into the adequacy of LabMD's information security practices in January 2010, after a LabMD file had been discovered on a peer-to-peer ("P2P") file sharing network.⁵ The file, which Petitioners call the "1,718 File" because it is 1,718 pages long, is a spreadsheet of health insurance billing information for uro pathology and microbiology medical tests of around 9,000 patients. It contains highly sensitive information about these consumers, including:

- Name;
- Social Security Number;
- Date of birth;
- Health insurance provider and policy number; and
- Standardized medical treatment codes.⁶

Such information can be misused to harm consumers.

The purpose of the investigation is to determine whether Petitioners violated the FTC Act by engaging in deceptive or unfair acts or practices relating to privacy or information security. The inquiry is authorized by Resolution File No. P954807, which provides for the use of compulsory process in investigations of potential Section 5 violations involving "consumer privacy and/or data security."

would have to be filed should be calculated from the date on which you receive the original letter by courier delivery.

⁴ *Id.*

⁵ P2P programs allow users to form networks with others using the same or a compatible P2P program. Such programs allow users to locate and retrieve files of interest to them that are stored on computers of other users on the networks.

⁶ LabMD Pet., Ex. C, at Fig. 4. Because the LabMD and Daugherty Petitions make the same arguments (the Petitions differ only in details about the submitter), we generally cite only to LabMD's Petition.

The investigation began with voluntary information requests for documents and information about LabMD's information security policies, procedures, practices, and training generally, as well as information about security incidents, including, but not limited to, the discovery of the 1,718 File on P2P networks. In response, LabMD produced hundreds of pages of documents, including supplements and responses to follow-up questions. To complete the investigation, staff requested issuance of CIDs to LabMD and Michael J. Daugherty, LabMD's President.

The Commission issued the CIDs on December 21, 2011. Both require testimony relating to information security policies, practices, training, and procedures. They also include a limited number of interrogatories that require Petitioners to identify documents used by the witnesses to prepare for their testimony.⁷ The LabMD CID also includes a single document request asking for only those documents that were both identified in response to the CID's interrogatories and had not been previously produced to staff.⁸

Petitioners seek to quash or limit the CIDs because, they claim, the CIDs "appear to be premised on" the download of the 1,718 File (hereinafter, the "File disclosure").⁹ Their principal objection relates to the merits of the investigation. In particular, they contend (without citing any authority) that the Commission must have a "justifiable" belief that a law violation has occurred before it can issue CIDs, and that the File disclosure cannot support such a belief. They claim that the File disclosure occurred not because LabMD failed to implement reasonable and appropriate security measures, but because the company was the victim of an illegal intrusion conducted by Tiversa (a P2P information technology and investigation services company) and Dartmouth College faculty using Tiversa's powerful P2P searching technology.¹⁰ Further, Petitioners argue that no actual harm to consumers resulted from the File disclosure.¹¹ Accordingly, they

⁷ LabMD Pet., Ex. A.

⁸ LabMD Pet., Ex. A.

⁹ LabMD Pet., at 1.

¹⁰ Petitioners claim that in the course of a Department of Homeland Security-funded research project, Professor M. Eric Johnson of Dartmouth College's Tuck School of Business and Tiversa used Tiversa's P2P searching technology to search for and then download the file. LabMD Pet., at 3-4, 7, & Ex. F, at 10-12.

¹¹ The Petitions claim that there is no allegation of actual consumer injury from the File disclosure. LabMD Pet., at 7.

contend that investigating either the File disclosure or the adequacy of LabMD's security practices is improper because no law violation can have occurred, and that the CIDs therefore should be quashed.¹²

As discussed below, these arguments are undermined by: (1) the obvious point that an investigation necessarily must precede assessment of whether there is reason to believe a law violation may have occurred (in any matter); (2) the scope of the authorizing resolution; and (3) the language of the FTC Act. The resolution authorizes use of compulsory process in an investigation to determine whether Petitioners engaged in deceptive or unfair practices related to privacy or security. Petitioners' focus on the File disclosure is misplaced – it may bear on the adequacy of LabMD's security practices under the FTC Act but does not establish the investigation's scope under the resolution.¹³ Further, in such an investigation Section 5 directs the Commission to consider whether security practices are unfair because they create a sufficient risk of harm, even if no harm has been reported.

Petitioners make two additional arguments in support of their Petitions. First, they argue that the resolution authorizing the CIDs did not provide them with sufficient notice of the purpose and scope of the investigation. Second, they argue that the FTC is without jurisdiction to pursue this investigation. Both of these additional arguments are equally without merit.

II. ANALYSIS

A. The applicable legal standards.

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as that inquiry is defined by the investigatory resolution.¹⁴

¹² LabMD Pet., at 7-8.

¹³ See, e.g., *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008) (confirming that the scope of an investigation authorized by Resolution P954807 properly included all of CVS' "consumer privacy and data security practices" (including its computer security practices) and could not be limited (as the company argued) to just known incidents of unauthorized disposal of paper documents in dumpsters).

¹⁴ *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have “a justifiable belief that wrongdoing has actually occurred,” as Petitioners claim.¹⁵ As the D.C. Circuit has stated, “The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one The requested material, therefore, need only be relevant to the *investigation* – the boundary of which may be defined quite generally, as it was in the Commission’s resolution here.”¹⁶ Agencies thus have “extreme breadth” in conducting their investigations,¹⁷ and “in light of [this] broad deference . . . , it is essentially the respondent’s burden to show that the information is irrelevant.”¹⁸

B. The CIDs satisfy the foregoing standards.

Petitioners argue that the CIDs are improper for several reasons. In particular, they claim no law violation could have occurred, by arguing that: (1) not even “perfect” security measures (let alone the reasonable security measure standard the Commission uses to determine whether a law violation may have occurred) could have prevented the File disclosure because Tiversa’s technology “can penetrate even the most robust network security,”¹⁹ and (2) no actual injury resulted from the File disclosure.

¹⁵ LabMD Pet., at 6. *See, e.g., Morton Salt*, 338 U.S. at 642-43 (“[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.”).

¹⁶ *Invention Submission*, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing *FTC v. Carter*, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

¹⁷ *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1517 (D.C. Cir. 1993) (citing *Texaco*, 555 F.2d at 882).

¹⁸ *Invention Submission*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) (“burden of showing that the request is unreasonable is on the subpoenaed party”). *Accord FTC v. Church & Dwight Co.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010).

¹⁹ LabMD Pet., at 7.

The Commission is not required, as a precondition to conducting a law enforcement investigation, to make a showing that it is likely that a law violation has occurred. The D.C. Circuit confirmed this point in *FTC v. Texaco, Inc.*, when it stated, “[I]n the pre-complaint stage, an investigating agency is under no obligation to propound a narrowly focused theory of a possible future case The court must not lose sight of the fact that the agency is merely exercising its legitimate right to determine the facts, and that a complaint may not, and need not, ever issue.”²⁰ Here, Petitioners seek to quash the CIDs by asserting that LabMD’s practices must have been reasonable under the FTC Act because the 1,718 File was retrieved using Tiversa’s powerful searching technology. Accepting this argument would prevent the Commission from exploring relevant issues bearing on reasonableness, such as, for example, whether the company’s security practices could have prevented the 1,718 File from being retrieved using the common P2P programs that are used by millions of computer users each day or whether there were readily available security measures LabMD did not implement that would have prevented even Tiversa’s technology from successfully retrieving the file. Although such evidence (if it exists at all) could undermine their reasonableness claim, Petitioners nonetheless argue that the Commission cannot use CIDs to investigate whether the evidence exists unless it already has reason to believe it does exist. For this reason, Petitioners’ argument that the strength of Tiversa’s P2P searching technology precludes the possibility that a law violation occurred, regardless of the state of LabMD’s security, must fail.

Similarly, Petitioners’ assertion that no law violation can have occurred because no actual harm has been shown also fails because, under Section 5, a failure to implement reasonable security measures may be an unfair act or practice if the failure is *likely* to cause harm. No showing of actual harm is needed.²¹

Both arguments conflate the purpose of a CID with the purpose of a future potential complaint. A CID can only compel information necessary for an investigation, and the investigation may or may not result in allegations of a law violation.²²

²⁰ 555 F.2d 862, 874 (D.C. Cir. 1977). This holding from *Texaco* has been repeatedly reaffirmed, most recently in *FTC v. Church & Dwight*, 747 F. Supp. 2d 3, 6, *aff’d*, 2011 U.S. App. LEXIS 24587 (D.C. Cir. Dec. 13, 2011).

²¹ 15 U.S.C. § 45(n) (an unfair practice is one that “causes or *is likely to cause* substantial injury to consumers”); *see also* FTC Policy Statement on Unfairness, 104 F.T.C. 949, 1073 & n.15 (1984).

²² Petitioners also argue that the CIDs are improper for other reasons. They claim that because security issues posed by P2P programs were common (according to Tiversa), such issues could not constitute an unfair or deceptive practice in violation of the FTC

Additionally, Petitioners have claimed that the CIDs are burdensome, but they have not come forward with any support for these assertions. Instead, they make only bald statements that the CIDs are “highly burdensome,” “unduly burdensome,” “costly and burdensome,” and “deeply burdensome.”²³ Having offered no factual information about the alleged burdens of complying with the CIDs, Petitioners have not sustained their burden to demonstrate that the CIDs are unduly burdensome.²⁴

Such a showing would be difficult here in any event. Notwithstanding Petitioners’ description, the CIDs call primarily for testimony, not documents. Thus, it seems unlikely that compliance would require large-scale or time-consuming document production.

Act. LabMD Pet., at 7-8 & n.34. This argument is unavailing. The fact that a particular practice may be pervasive or widespread has no bearing on whether the FTC may investigate it as also deceptive or unfair. Indeed, accepting Petitioners’ argument would confine the FTC to investigating only those activities that were rare or uncommon, thus crippling the agency’s law enforcement mission. Along the same lines, Petitioners contend that the risks of P2P technology, and the resulting potential liabilities to businesses, were not known in 2008, when the File disclosure occurred. In support of this claim, they assert that the FTC did not notify businesses or publish guidance about P2P until 2010. LabMD Pet., at 8. In fact, many, including the FTC, warned about the risks presented by P2P programs years before the File disclosure occurred. *See, e.g.*, FTC Staff Report, “Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues” (June 2005), available at <http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>; Prepared Statement of the Federal Trade Commission Before The Committee on Oversight and Government Reform, United States House of Representatives (July 24, 2007) (discussing P2P programs and risks), available at <http://www.ftc.gov/os/testimony/P034517p2pshare.pdf>.

²³ LabMD Pet., at 7, 9, & 10.

²⁴ *See, e.g., Texaco*, 555 F.2d at 882 (“The burden of showing that the request is unreasonable is on the subpoenaed party.”) (citing *United States v. Powell*, 379 U.S. 48, 58 (1964)); *accord EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986) (subpoena is enforceable absent a showing by recipient that the requests are unduly burdensome); *FTC v. Standard American, Inc.*, 306 F.2d 231, 235 (3d Cir. 1962) (recipient has responsibility to show burden and must make “a record . . . of the measure of their grievance rather than ask [the court] to assume it”); *In re Nat’l Claims Serv., Inc.*, 125 F.T.C. 1325, 1328-29 (1998) (FTC ruling that petition to quash must substantiate burden with specific factual detail).

Furthermore, to the extent that the CIDs call for narrative responses, they merely require Petitioners to identify documents related to the requested testimony. In fact, there is only one specification that requires the production of documents, and even that specification is limited to documents identified in response to the interrogatories to the extent they were “not already been produced to the FTC.”²⁵

Finally, Petitioners, without explaining its relevance, contend that the timing of the CIDs is “troubling,” coming after LabMD’s conduct had been reviewed by two congressional committees, and after LabMD filed suit against Tiversa and others alleging conversion and trespass, among other violations, based on the File disclosure in 2008.²⁶ Though Petitioners seem to believe that there is some connection between their rejection of Tiversa’s offer to provide LabMD with information security services, their subsequent lawsuit, and the FTC’s investigation, the chronology of the investigation does not support such a conclusion. The FTC first contacted LabMD for information in January 2010, well before LabMD filed its lawsuit against Tiversa in October 2011.²⁷ Moreover, the claim that LabMD’s conduct was reviewed by congressional committees does not appear to be based on evidence presented in the Petitions. Although Petitioners have attached as exhibits three instances of congressional testimony by Tiversa, none identifies LabMD by name or discusses the specifics of the File disclosure.

C. The resolution provides sufficient notice of the purpose and scope of the FTC’s investigation.

Under the FTC Act, a CID is proper when it “state[s] the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.”²⁸ It is well-established that the resolution authorizing the process provides the requisite statement of the purpose and scope of the investigation,²⁹

²⁵ LabMD Pet., Ex. A.

²⁶ LabMD Pet., at 9 & Ex. F.

²⁷ We note further that this suit came more than three years after the solicitations Petitioners complain of in their Petitions. LabMD Pet., Ex. F, at 1, 17-23.

²⁸ 15 U.S.C. § 57b-1(c)(2).

²⁹ *Invention Submission*, 965 F.2d at 1088; *accord Texaco*, 555 F.2d at 874; *FTC v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980); *FTC v. Anderson*, 631 F.2d 741, 746 (D.C. Cir. 1979).

and also that the resolution may define the investigation generally, need not state the purpose with specificity, and need not tie it to any particular theory of violation.³⁰

Despite this, Petitioners object that Resolution File No. P954807 did not provide sufficient notice of the purpose and scope of the investigation, and they further claim that this resolution is inadequate under the standard developed by the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980).³¹

Petitioners' first argument reads the governing standard too narrowly. Resolution File No. P954807 authorizes the use of compulsory process:

to determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.³²

This general statement of the purpose and scope of the investigation is more than sufficient under the standard for such resolutions, and courts have enforced compulsory process issued under similarly broad resolutions.³³

Petitioners' reliance on *Carter* is also misplaced. While *Carter* held that a bare reference to Section 5, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue in that case, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further

³⁰ *Invention Submission*, 965 F.2d at 1090; *Texaco*, 555 F.2d at 874 & n.26; *FTC v. Nat'l Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (citing *EPA v. Alyeska Pipeline Serv. Co.*, 836 F.2d 443, 477 (9th Cir. 1988)).

³¹ LabMD Pet., at 10-12.

³² LabMD Pet., Ex. A.

³³ See *FTC v. Nat'l Claims Serv.*, 1999 WL 819640, at *2 (finding omnibus resolution referring to FTC Act and Fair Credit Reporting Act sufficient); *FTC v. O'Connell Assoc., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution). The Commission has repeatedly rejected similar arguments about such omnibus resolutions. See, e.g., *Firefighters Charitable Found.*, No. 102-3023, at 4 (Sept. 23, 2010); *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

related it to the subject matter of the investigation.³⁴ With this additional information, the Court felt “comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit”³⁵

The resolution here, like the one in *Carter*, does not cite solely to Section 5, but also recites the subject matter of the investigation: “deceptive or unfair acts or practices related to consumer privacy and/or data security.” Since the resolution here discloses the subject matter of the investigation in addition to invoking Section 5, the resolution provides notice sufficient under *Carter* of the purpose and scope of the investigation.

As a final note, the history of the investigation itself undermines Petitioners’ argument that the present CIDs do not sufficiently advise them of the nature and scope of the investigation. Petitioners have been under investigation since January 2010 and have engaged in repeated discussions with staff. At no point have Petitioners indicated they did not understand the purpose or scope; in fact, Petitioners have already produced hundreds of pages of documents in response to staff requests. Moreover, the Petitions under consideration here present highly detailed and factual arguments going to the very merits of the investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners.³⁶

D. Petitioners’ challenge to the FTC’s regulatory authority is premature and without basis.

Petitioners’ final argument is that the FTC lacks jurisdiction to conduct the instant investigation.³⁷ Petitioners assert that LabMD is a health care company and that the

³⁴ *Carter*, 636 F.2d at 788.

³⁵ *Id.*

³⁶ *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) (“[T]he notice provided in the compulsory process resolutions, CIDs and other communications with Petitioner more than meets the Commission’s obligation of providing notice of the conduct and the potential statutory violations under investigation.”).

³⁷ Petitioners also claim that the resolution does not meet the requirements established by the FTC’s Operating Manual. *LabMD Pet.*, at 10. As discussed above, by disclosing the statutory basis and subject matter of the investigation, the resolution does provide notice as required by the Operating Manual. That said, the Operating Manual, by its own terms, is advisory. It is not a “basis for nullifying any action of the Commission or the staff.”

information disclosed in the 1,718 File is protected health information (“PHI”) under the Health Insurance Portability and Accountability Act (“HIPAA”). Accordingly, they contend, the adequacy of their security practices with respect to this information is subject to the exclusive jurisdiction of HHS.³⁸

As an initial matter, it is well-established that challenges to the FTC’s jurisdiction are not properly raised through challenges to investigatory process. As the D.C. Circuit stated: “Following *Endicott* [*Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (1943)], courts of appeals have consistently deferred to agency determinations of their own investigative authority, and have generally refused to entertain challenges to agency authority in proceedings to enforce compulsory process.”³⁹ The reasons for such a rule are obvious. If a party under investigation could raise substantive challenges in an enforcement proceeding, before the agency has obtained the information necessary for its case – essentially requiring the FTC to litigate an issue before it can learn about it – then the FTC’s investigations would be foreclosed or substantially delayed.⁴⁰ Thus, Petitioners’ basic challenge to the FTC’s jurisdiction is premature and will not support quashing the instant CIDs.

In any event, the claim that HHS has exclusive jurisdiction to investigate privacy and data security issues involving PHI is without basis. Petitioners essentially invoke the doctrine of implied repeal to assert that HIPAA and its Privacy and Security Rules displace FTC jurisdiction. But implied repeal is “strongly disfavored,” for two reasons.⁴¹ First, courts have recognized that agencies may have overlapping or concurrent jurisdiction, and thus that the same issues may be addressed and the same parties

Operating Manual, § 1.1.1.1. *See also* *FTC v. Nat’l Bus. Consultants, Inc.* 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶68,984, at *29 (E.D. La. March 19, 1990).

³⁸ LabMD Pet., at 12-13.

³⁹ *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (citing *United States v. Sturm, Ruger & Co.*, 84 F.3d 1, 5 (1st Cir. 1996)); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 468-73 (2d Cir. 1996); *EEOC v. Peat, Marwick, Mitchell & Co.*, 775 F.2d 928, 930 (8th Cir. 1985); *Donovan v. Shaw*, 668 F.2d 985, 989 (8th Cir. 1982); *FTC v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979); *accord Oklahoma Press Publ’g Co. v. Walling*, 327 U.S. 186, 213-14 (1946).

⁴⁰ *Texaco*, 555 F.2d at 879.

⁴¹ *Galliano v. United States Postal Serv.*, 836 F.2d 1362, 1369 (D.C. Cir. 1988).

proceeded against simultaneously by more than one agency.⁴² Second, courts rarely hold that one federal statute impliedly repeals another because “when two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective.”⁴³ Thus, repeals by implication will only be found where the Congressional intent to effect such a repeal is “clear and manifest.”⁴⁴

Petitioners can point to no such “clear or manifest” evidence that Congress intended HIPAA or its rules to displace the FTC Act. The authority Petitioners cite for the proposition that HHS has exclusive jurisdiction does not address such repeal.⁴⁵ To the contrary, there is ample evidence against such implied repeal. For one, the same authority cited by Petitioners – the preamble to the Privacy Rule – expressly provides that entities covered by that Rule are “also subject to other federal statutes and regulations.”⁴⁶ Also, this preamble includes an “Implied Repeal Analysis,” which is silent as to any implied repeal of the FTC Act.⁴⁷ Recent legislation shows that, if anything, Congress intended the FTC and HHS to work collaboratively to address potential privacy and data security risks related to health information. The American Recovery and Reinvestment Act of 2009, for instance, required HHS and the FTC to develop harmonized rules for data breach notifications by HIPAA-covered and non-HIPAA-covered entities, respectively. *See* 74

⁴² *FTC v. Cement Inst.*, 333 U.S. 683, 694 (1948); *see also Texaco*, 555 F.2d at 881 (“[T]his is an era of overlapping agency jurisdiction under different statutory mandates.”); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986). Because agencies have overlapping jurisdiction, they often work together. For instance, the FTC and HHS collaborated on the investigation of CVS Caremark Corporation. *See CVS Caremark Corp.*, No. 072-3119, at 7 (Aug. 6, 2008).

⁴³ *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976) (quoting *Morton v. Mancari*, 417 U.S. 535, 551 (1974)).

⁴⁴ *Id.* at 154.

⁴⁵ LabMD Pet., at 12 (citing 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000)). This Federal Register notice is the Notice of Public Rulemaking for the Privacy and Security Rules under HIPAA. The excerpt cited by Petitioners does not address the scope of HHS’ enforcement jurisdiction, but rather discusses the delegation of enforcement authority from the Secretary of HHS to HHS’ Office for Civil Rights. 65 Fed. Reg. 82,472 (Dec. 28, 2000).

⁴⁶ 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000).

⁴⁷ *Id.* at 82,481-487.

Fed. Reg. 42,962, 42,962-63 (Aug. 25, 2009). Thus, HIPAA and its Rules do not serve to repeal FTC jurisdiction, which is overlapping and concurrent to HHS’.

This is particularly appropriate where, as here, the consumer information at issue included more than just health information. The consumer information exposed in the 1,718 File also included names, Social Security numbers, and dates of birth. While this information can be considered PHI under HIPAA when combined with health information, the information clearly exposes consumers to the risk of identity theft and is exactly the kind of sensitive personal information that the Commission is charged with protecting under Section 5 of the FTC Act and other statutes. Petitioners have provided no proper basis to challenge the investigation as an exercise of the Commission’s jurisdiction under these authorities.

III. CONCLUSION AND ORDER

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** LabMD, Inc.’s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Michael J. Daugherty’s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6); and

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must now be produced on or before May 11, 2012.

By direction of the Commission.

Donald S. Clark
Secretary

**FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL
DAUGHERTY**

PETITION EXHIBIT 7

**LabMD, Inc's and Michael J. Daugherty's Request for
Review by the Full Commission (Apr. 25, 2012)**



2030 Powers Ferry Drive • Building 500 • Suite 520 • Atlanta, Georgia 30339 • sfusco@labmd.org • 678-443-2343

April 25, 2012

Via Facsimile, Email and Hand Delivery

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

Re: *LabMD, Inc. and Michal J. Daugherty*

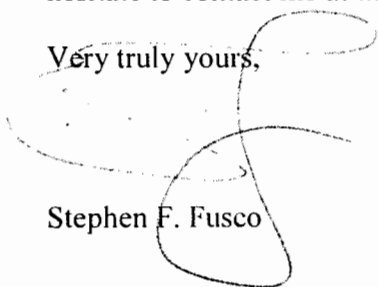
Dear Mr. Clark:

I am writing to you as counsel to LabMD, Inc. and Michael J. Daugherty. Please be advised that we are requesting a review of the LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand by the full Commission pursuant to 16 CFR 2.7. We are also requesting a full hearing regarding this matter. Please advise as to when the full hearing will occur so we can make travel plans to testify at the hearing.

In light of this request for full Commission review, we also request that the Federal Trade Commission ("FTC") stay the CIDs issued to the parties by the FTC on December 21, 2011. Please advise at the earliest possible date as to this request for a stay.

Additionally, please change your records to list me as counsel of record on behalf of LabMD, Inc. and Mr. Michael J. Daugherty. Please direct all future correspondence to my at the above-referenced address. If you should have any questions, please do not hesitate to contact me at the number listed above.

Very truly yours,


Stephen F. Fusco

cc: Claudia Callaway
Christina J. Grigorian
Mr. Michael J. Daugherty

FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL DAUGHERTY

PETITION EXHIBIT 8

**Commission Letter Affirming the Ruling, By Commissioner Brill, Denying the Petitions To Limit or Quash Filed by LabMD, Inc. and Michael J. Daugherty
(June 21, 2012)**



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

June 21, 2012

BY E-MAIL AND COURIER DELIVERY

Stephen F. Fusco, Esq.
LabMD
2030 Powers Ferry Drive
Building 500, Suite 520
Atlanta, GA 30339
sfusco@labmd.org

RE: *Request for Full Commission Review of Denial of Petitions to Limit or Quash the Civil Investigative Demand by LabMD, Inc. and Michael J. Daugherty (FTC File No. 1023099)*

Dear Mr. Fusco:

This letter advises you of the Commission's disposition of LabMD, Inc.'s and Michael J. Daugherty's request dated April 25, 2012, that the full Commission review the denial of their petition to limit or quash civil investigative demands.

The Commission issued the CIDs to LabMD and Mr. Daugherty on December 21, 2011. LabMD and Mr. Daugherty filed petitions to limit or quash the CIDs, which were received by the Commission on January 10, 2012. On April 20, 2012, Commissioner Brill directed the issuance of a letter denying both petitions and directing both petitioners to comply by May 11, 2012. That deadline was extended to June 8, 2012 due to emergency circumstances that you brought to the Commission's attention.²¹

The Commission affirms the ruling denying the petitions to limit or quash the civil investigative demands. The Commission has independently reviewed LabMD and Mr. Daugherty's petitions to limit or quash the CIDs, and their requests for full Commission review. The Commission has also reviewed the letter ruling issued by the Commission at the direction of Commissioner Brill, and hereby affirms that ruling, finding its conclusions to be valid and correct.

²¹ On April 30, 2012, you contacted the Commission's Office of the Secretary to request additional time to comply with the CID due to emergency circumstances. By letter dated May 7, 2012, the Commission modified the date to June 8, 2012.

Commissioner Rosch generally agrees with the Commission's decision to enforce the CIDs, but dissents from this ruling to the extent it permits staff to rely on a LabMD document found on a peer-to-peer file sharing network, out of concern about petitioners' allegations that a third party located this document through wrongdoing and for financially-motivated reasons. In this ruling, we make no findings of fact regarding that third party's conduct or the admissibility of this document, nor do we need to do so. In upholding the CIDs, the Commission allows staff to continue to use pertinent information—including information from or concerning any LabMD documents made available to users of peer-to-peer file-sharing networks and accessed by any third party—to conduct its data security investigation. Indeed, in our data security investigations, the Commission often uses information obtained by third parties concerning security vulnerabilities of entities that maintain substantial amounts of personal information. Although we understand petitioners have alleged that the third party in question has a financial incentive to use its patented monitoring tool to find information that has been improperly disclosed on peer-to-peer file sharing networks, that does not overcome the Commission's compelling public interest in seeking to protect consumers' sensitive health data by pursuing this investigation through all lawful means, including the use of this document.

The April 25, 2012 request for full Commission review also requested a hearing on the denial of the petitions. The FTC Rule governing petitions to quash or limit, 16 C.F.R. § 2.7, does not provide for such a hearing, however, and accordingly, this request will be denied.

For the forgoing reasons,

IT IS ORDERED THAT the April 20, 2012 letter ruling is **AFFIRMED**;

IT IS FURTHER ORDERED THAT LabMD's and Mr. Daugherty's request for a hearing is **DENIED**;

IT IS FURTHER ORDERED THAT Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6)(2012); and

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must be produced on or before June 8, 2012.

By direction of the Commission, Commissioner Rosch dissenting, and Commissioner Ohlhausen not participating.

Donald S. Clark
Secretary

Dissenting Statement of Commissioner J. Thomas Rosch
Petitions of LabMD, Inc. and Michael J. Daugherty
to Limit or Quash the Civil Investigative Demands

FTC File No. 1023099
June 21, 2012

I dissent from the Commission's vote affirming Commissioner Brill's letter decision, dated April 20, 2012, that denied the petitions of LabMD, Inc. and Michael J. Daugherty to limit or quash the civil investigative demands.

I generally agree with Commissioner Brill's decision to enforce the document requests and interrogatories, and to allow investigational hearings to proceed. As she has concluded, further discovery may establish that there is indeed reason to believe there is Section 5 liability regarding petitioners' security failings *independent* of the "1,718 File" (the 1,718 page spreadsheet containing sensitive personally identifiable information regarding approximately 9,000 patients) that was originally discovered through the efforts of Dartmouth Professor M. Eric Johnson and Tiversa, Inc. In my view, however, as a matter of prosecutorial discretion under the unique circumstances posed by this investigation, the CIDs should be limited. Accordingly, without reaching the merits of petitioners' legal claims, I do not agree that staff should further inquire – either by document request, interrogatory, or investigational hearing – about the 1,718 File.

Specifically, I am concerned that Tiversa is more than an ordinary witness, informant, or "whistle-blower." It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering

investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. In my view, while there appears to be nothing *per se* unlawful about this evidence, the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

**FEDERAL TRADE COMMISSION v. LABMD, INC., AND MICHAEL
DAUGHERTY**

PETITION EXHIBIT 9

**Letter from Counsel for LabMD, Inc. and
Michael J. Daugherty (June 29, 2012)**



2040 Powers Ferry Drive • Building 500 • Suite 520 • Atlanta, Georgia 30339 • fusco@labmd.org • 678-443-2311

June 29, 2012

Mr. Alain Sheer
Senior Attorney, Division of Privacy and Identity Protection
Bureau of Consumer Protection
United States Federal Trade Commission
Washington, D.C. 20580

Dear Alain:

I am writing in response to your June 27, 2012 correspondence following your impromptu call. As the call was rather last minute, I did not take a verbatim transcription of our conversation and cannot attest to your characterization of the conversation on the phone. In order to avoid this issue in the future, as it appears that the FTC is concerned with certain representations made by LabMD, Inc. and Mr. Michael J. Daugherty (the "Parties"), I respectfully request that all future communications be in written form.

With respect to the Civil Investigative Demands ("CID") issued to the Parties on December 21, 2011, I refer you to their respective Motions to Quash which outline, in great detail, the factual and legal basis upon which the Parties believe the CIDs are invalid and illegal. For purposes of this letter, the Parties renew and incorporate their arguments regarding the invalidity of the CIDs herein as though stated in their entirety. As such, it is not possible to make any representations about the CIDs or compliance with the same since they are a nullity by law.

I trust this letter addresses all of your questions.

Sincerely,

Stephen F. Fusco, Esq.

A handwritten signature in black ink, appearing to read "S. Fusco".

determine whether respondents engaged in “unfair or deceptive acts or practices” in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, by employing unreasonable data security measures that resulted in patients’ sensitive personal information being available to the public on easily accessible peer-to-peer networks.

While LabMD and Mr. Daugherty have provided FTC staff with some responsive information and documents in response to voluntary access requests, they have persisted in refusing to comply with the CIDs, which, in principal part, require them to appear and testify at investigational hearings.¹ The full Commission denied respondents’ administrative petitions to quash, concluding that their arguments were meritless. The failure of LabMD and Mr. Daugherty to respond to the CIDs continues to greatly impede the ongoing investigation.

This proceeding is properly instituted by a petition and order to show cause (rather than by complaint and summons) and is summary in nature; discovery or evidentiary hearings are granted only upon a showing of exceptional circumstances.

See, e.g., FTC v. Carter, 636 F.2d 781, 789 (D.C. Cir. 1980); *FTC v. MacArthur*, 532

¹ The CIDs include a limited number of interrogatories directing LabMD and Mr. Daugherty to identify documents they used in preparing for their testimony. Additionally, the CID to LabMD requires it to produce any documents identified in response to the interrogatories, if they had not already been produced. Petition Exhibits 2 & 3 (hereinafter “Pet. Exh.”).

F.2d 1135, 1141-42 (7th Cir. 1976); *Genuine Parts Co. v. FTC*, 445 F.2d 1382, 1388 (5th Cir. 1971);² *see also United States v. Markwood*, 48 F.3d 969, 981-82 (6th Cir. 1995); *Appeal of FTC Line of Business Report Litigation*, 595 F.2d 685, 704-05 (D.C. Cir. 1978). As shown below, the instant CIDs were lawfully issued, are not unduly burdensome, and the testimony and information sought are plainly relevant to the Commission's investigation. The Commission, accordingly, respectfully requests that this Court direct LabMD and Mr. Daugherty to appear and show cause why they should not fully comply, and thereafter enter its own order enforcing the CIDs. *See, e.g., United States v. Florida Azalea Specialists*, 19 F.3d 620, 623-24 (11th Cir. 1994).

JURISDICTION

The Commission is an administrative agency of the United States, organized and existing pursuant to the FTC Act, 15 U.S.C. § 41 *et. seq.* The Commission is authorized by Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), to prohibit, *inter alia*, “unfair or deceptive acts or practices” in or affecting commerce. The authority of the Commission to issue a CID, and the jurisdiction and venue of this court to enter an order enforcing it, are conferred by Section 20(c) of the FTC Act, 15 U.S.C. § 57b-

² Cases decided by the former Fifth Circuit prior to the close of business on September 30, 1981, are binding precedent. *Bonner v. City of Prichard*, 661 F.2d 1206, 1209 (11th Cir. 1981).

1(c), which empowers the Commission to issue CIDs to require, *inter alia*, oral testimony, the production of documentary evidence, and responses to written interrogatories. Sections 20(e) and (h) of the FTC Act, 15 U.S.C. §§ 57b-1(e) and (h), authorize the Commission to invoke the aid of the district courts to enforce a CID in any jurisdiction in which the recipient of a CID “resides, is found, or transacts business.” Section 20(e) also authorizes the Commission to seek enforcement of a CID in its own name using its own counsel. 15 U.S.C. § 57b-1(e).

In this case, venue and jurisdiction are proper under Section 20(e) because LabMD and Mr. Daugherty are found, and transact business, in Atlanta, Georgia, which is within this District. Pet. Exh. 1 ¶¶ 1, 3.

STATEMENT OF FACTS

1. Background

Respondent LabMD is a Georgia corporation, with its headquarters at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339. Pet Exh. 1 ¶ 3. LabMD provides medical testing services and transacts business in various States throughout the United States. *Id.* Respondent Michael J. Daugherty is the owner and president of LabMD. *Id.* ¶ 1. LabMD and Mr. Daugherty are engaged in, and their business affects, “commerce,” as that term is defined in Section 4 of the FTC Act, 15

U.S.C. § 44.

In 2009, FTC staff became concerned about reports that some consumers' personally-identifiable and highly sensitive health information had become available on publicly accessible peer-to-peer ("P2P") file sharing networks. Pet. Exh. 1 ¶ 4. Indeed, in May 2009, the risks of making such information available on P2P networks was detailed in congressional testimony by Robert Boback, CEO of Tiversa, Inc., a data security and investigations firm that monitors P2P networks for its clients.³ See Pet. Exh. 4 (LabMD Pet. to Quash), Exh. C. The gist of the testimony was that Tiversa had found millions of files from consumers, businesses, and government agencies exposed on P2P networks, including tax returns, Social Security numbers, credit card numbers, and health insurance and medical information. *Id.* Tiversa made these discoveries in the course of a collaboration with Professor M. Eric Johnson of Dartmouth College on a research project funded by the U.S. Department of Homeland

³ *Legis. Hearing on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act Before the Subcomm. On Commerce, Trade, and Consumer Protection of the H. Comm. On Energy & Commerce, 111th Cong. (May 5, 2009) (statement of Robert Boback, CEO, Tiversa, Inc.), available at http://democrats.energycommerce.house.gov/Press_111/20090505/testimony_boback.pdf.*

Security.⁴

FTC staff initiated an inquiry to determine whether the disclosures of consumers' personal information were attributable to failures to employ reasonable data security measures in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or whether they violated any other statutes or regulations enforced by the Commission. Pet Exh. 1 ¶ 4. As part of this inquiry, Commission staff consulted with third parties, including Tiversa. *Id.*

In the fall of 2009, FTC staff, using compulsory process, obtained copies of a number of electronic files that were located on P2P networks and that contained sensitive information. Pet. Exh. 1 ¶ 5. Included among those files was a spreadsheet (the "1,718 File") that contained personally-identifiable information and sensitive health information for about 9,000 LabMD patients, including patient names, Social Security numbers, birth dates, health insurance provider names and policy numbers,

⁴ Professor Johnson described his findings in an academic paper in which he explained, "We found multiple files from major health-care firms that contained private employee and patient information for literally tens of thousands of individuals, including addresses, Social Security Numbers, birth dates, [] treatment billing information . . . medical diagnoses and psychiatric evaluations." M. Eric Johnson, *Data Hemorrhages in the Health-Care Sector*, Presentation at Financial Cryptography and Data Security Conference (Feb. 22-25, 2009), available at <http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/JohnsonHemorrhagesFC09Proceedingd.pdf>. See Pet. Exh. 4, Exh. C, p. 2.

and medical treatment codes. *Id.*

In 2010, after reviewing the 1,718 File and other information and consulting with other law enforcement agencies, FTC staff expanded the investigation by issuing voluntary access requests to a number of different entities, including LabMD. *Id.* ¶ 6. The purpose of those requests was to assist FTC staff in determining whether those entities may have violated laws enforced by the Commission (*e.g.*, the FTC Act, 15 U.S.C. § 45(a), and the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-09) by failing to use reasonable and appropriate security measures to safeguard sensitive health and personally-identifiable information. Pet. Exh. 1 ¶ 6.

While LabMD and Mr. Daugherty provided some information and documents in response to the access letter and follow-up requests, FTC staff determined that further and formal inquiry was necessary. *Id.* ¶¶ 6-7. Accordingly, on December 21, 2011, the Commission issued CIDs that directed LabMD and Mr. Daugherty to appear at investigational hearings and to testify regarding, *inter alia*, (i) LabMD's information security practices; (ii) any security risks, vulnerabilities, and incidents where LabMD's documents might have been accessed or disclosed without authorization; and (iii) the specific responsibilities of Mr. Daugherty and other LabMD personnel in adopting and monitoring security practices and responding to

security incidents.⁵ Pet. Exhs. 2, 3. The CIDs also included a limited number of interrogatories that directed LabMD and Mr. Daugherty to identify documents they used in preparing their testimony. *Id.* Additionally, the Commission directed LabMD to produce any documents identified in its responses to the interrogatories, if they had not previously been produced. Pet. Exh. 2.

2. Administrative Petitions to Quash

On January 10, 2012, LabMD and Mr. Daugherty, pursuant to FTC Rule of Practice 2.7(d), 16 C.F.R. § 2.7(d), filed substantially similar administrative petitions to quash the CIDs. Pet. Exhs. 4, 5. On April 20, 2012, FTC Commissioner Brill, acting pursuant to authority delegated by the full Commission, issued a letter ruling denying the petitions. Pet. Exh. 6.

⁵ The CIDs were issued pursuant to a Commission resolution that authorized the use of formal compulsory process

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.

Resolution Directing Use of Compulsory Process in Nonpublic Investigation, File No. P954807 (January 3, 2008); *see also* Pet. Exhs. 2, 3.

In petitioning to quash the CIDs, respondents' principal argument was that Tiversa and Professor Johnson had downloaded the 1,718 File without authorization. *See, e.g.*, Pet. Exh. 4, at 2-5, 7-9. Consequently, respondents argued, they could not have violated any of the prohibitions of the FTC Act.⁶ Commissioner Brill ruled that this contention was premature. She explained that the Commission has a "legitimate right to determine the facts, and [] a complaint may not, and need not, ever issue." Pet. Exh. 6, at 6 (quoting *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977)). Thus, she concluded, the Commission was entitled to investigate (i) "whether [LabMD's] security practices could have prevented the 1,718 File from being retrieved using the common P2P programs that are used by millions of computer users each day," and (ii) whether LabMD failed to implement "readily available security measures" that would have prevented even a user with "powerful searching technology" from downloading the file. *Id.*⁷

⁶ On August 15, 2012, this Court dismissed LabMD's private action against Tiversa, Dartmouth College, and Professor Johnson on the grounds that personal jurisdiction was lacking. *See LabMD, Inc. v. Tiversa, Inc. et al.*, No. 1:11-cv-04404-JOF (N.D. Ga.).

⁷ Commissioner Brill also rejected respondents' contention that the Commission, in issuing its CIDs, was retaliating against LabMD for filing a civil suit against Tiversa. Commissioner Brill explained that the timeline of the investigation – *i.e.*, "[t]he FTC first contacted LabMD for information in January 2010, *well before* LabMD filed its civil suit against Tiversa in October 2011" – demonstrated

As for respondents' challenge to the Commission's authority to inquire into respondents' data security practices, Pet. Exh. 4, at 12-13, Commissioner Brill ruled that there was no support for their contention that the FTC's investigatory authority with respect to sensitive health information had been supplanted by the Health Insurance Portability and Accountability Act ("HIPAA") and its implementing rules. Indeed, she noted, the Preamble to HHS's Privacy Rule acknowledges specifically that entities covered by the Rule are "also subject to other federal statutes and regulations." *Id.* at 12 (citing 65 Fed. Reg. 82,462, 82,481-487 (Dec. 28, 2000)).

Commissioner Brill also rejected respondents' claims of undue burden, noting that the CIDs call "primarily for testimony" rather than a "large-scale or time-consuming document production" and that respondents had offered nothing to support their claims of burden other than "bald statements." Pet. Exh. 6, at 7-8. Commissioner Brill rejected as well the contention that the Commission's investigatory resolution was overly broad. Pet. Exh. 4, at 10-12. Citing longstanding precedent, she explained that a "resolution may define the investigation generally, need not state the purpose with specificity, and need not tie it to any particular theory

conclusively that respondents' allegations were meritless. Pet. Exh. 6, at 8 (emphasis added).

of violation.” Pet. Exh. 6, at 9 (citing *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992); *Texaco*, 555 F.2d at 874 & n.26).

3. Petition for Review by the Full Commission

On April 25, 2012, LabMD and Mr. Daugherty filed a petition for review by the full Commission. Pet. Exh. 7. On June 21, 2012, the Commission determined that Commissioner Brill’s rulings were “valid and correct,” denied the petition, and directed LabMD and Mr. Daugherty to comply. Pet. Exh. 8.⁸ The Commission held that notwithstanding LabMD’s assertion that Tiversa “has a financial incentive” to locate information “improperly disclosed” on P2P networks, the Commission has a “compelling interest in seeking to protect consumers’ sensitive health information through all lawful means,” including through use of the 1,718 File. *Id.*

On June 25, 2012, FTC staff contacted counsel for LabMD and Mr. Daugherty, Stephen F. Fusco, to discuss respondents’ plans to comply with the Commission

⁸ Commissioner Rosch “generally agree[d] with Commissioner Brill’s decision to enforce the document requests and interrogatories, and to allow investigational hearings to proceed.” Pet. Exh. 8, at 3. He noted, however, that Tiversa is a “commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations.” *Id.* For that reason, while observing that “there appears to be nothing *per se* unlawful about this evidence,” Commissioner Rosch would have directed FTC staff not to rely on the 1,718 File as a matter of “prosecutorial discretion.” *Id.* at 3-4.

orders. Pet. Exh. 1 ¶ 11. However, by letter dated June 29, 2012, LabMD and Mr. Daugherty renewed the objections raised in their unsuccessful petitions to quash and refused to make any representations regarding any plans to comply with the CIDs. Pet. Exh. 9. To date, LabMD and Mr. Daugherty have taken no steps to comply.

ARGUMENT

THE CIDS ARE LAWFUL, SEEK RELEVANT INFORMATION, AND ARE NOT UNDULY BURDENSOME

A. Standards for Enforcement of Agency Process

The standards for judicial enforcement of agency investigative process have long been settled. The court's role in a proceeding to enforce an agency's investigatory process is "sharply limited." *United States v. Florida Azalea Specialists*, 19 F.3d 620, 623 (11th Cir. 1994) (quoting *EEOC v. Kloster Cruise Ltd.*, 939 F.2d 920, 922 (11th Cir. 1991)). While "the court's function is neither minor nor ministerial, the scope of issues which may be litigated in a [compulsory process] enforcement proceeding must be narrow, because of the important governmental interest in the expeditious investigation of possible unlawful activity." *FTC v. Texaco, Inc.*, 555 F.2d 862, 872 (D.C. Cir. 1977) (*en banc*) (internal citation omitted). Thus, a district court must enforce agency process so long as (1) the inquiry is within the authority of the agency; (2) the demand is not too indefinite; and (3) the

information sought is reasonably relevant. *EEOC v. Tire Kingdom, Inc.*, 80 F.3d 449, 450 (11th Cir. 1996) (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *Florida Azalea*, 19 F.3d at 623); *see also Barton v. Parker*, No. Civ.A.1:01-CV-2004-J, 2001 WL 34049915, at *1 (N.D. Ga. Dec. 13, 2001).

As shown below, all the standards governing enforcement of the CIDs have been satisfied.

B. The Inquiry is Within the Commission's Authority

The Commission issued the instant CIDs in aid of an investigation into possible violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). The Commission authorized the use of such compulsory process in investigations such as this one by issuing a Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security on January 3, 2008. Pet. Exh. 2, at 3. According to the Resolution, the Commission seeks to determine whether persons, partnerships, corporations, or others have engaged in “unfair or deceptive acts or practices” relating to consumer privacy or data security in violation of Section 5 of the FTC Act, 15 U.S.C. § 45. *Id.* The Resolution “hereby resolves and directs that any and all compulsory process available to [the Commission] be used in connection with this investigation not to exceed five (5) years

from the date of issuance of this resolution.” *Id.*⁹

As the Commission explained in its ruling, Section 20 of the FTC Act gives the Commission ample authority to conduct the investigation and to issue CIDs in furtherance of the inquiry. *See* 15 U.S.C. § 57b-1; *see also* 16 C.F.R. § 2.7(a).¹⁰ The CIDs here seek the testimony of LabMD and Mr. Daugherty, answers to interrogatories identifying the documents they used to prepare for their testimony, and production of such documents, to the extent they have not already been produced. Pet. Exhs. 3, 4. All of this information is undisputedly “relating to” the subject of the investigation – whether LabMD and Mr. Daugherty failed to employ reasonable data security measures. 16 C.F.R. § 2.7(a). The CIDs were duly signed by a member of the Commission, as provided in the Commission’s rules. *Id.*

Respondents, in petitioning to quash the CIDs, have advanced the proposition that the Commission’s investigative resolution was overly broad. Pet. Exh. 4, at 10-

⁹ The purpose of an FTC investigation is defined by the investigative resolution that authorizes compulsory process. *Invention Submission*, 965 F.2d at 1087-88.

¹⁰ Section 2.7(a) of the Commission’s Rules of Practice provides, in relevant part: “The Commission or any member thereof may, pursuant to a Commission resolution, issue a . . . civil investigative demand directing the person named therein to appear before a designated representative at a designated time and place to testify or to produce documentary evidence, or both . . . or . . . to provide . . . answers to questions relating to any matter under investigation by the Commission.”

12. However, as the Commission explained in denying the petitions, a resolution need only describe the investigation in general terms and need not specifically state any particular theory of violation. Pet. Exh. 6, at 8-9; *see also Invention Submission*, 965 F.2d at 1090; *Texaco*, 555 F.2d at 874 & n.26. Indeed, courts have approved investigatory resolutions that are comparable to the resolution at issue in this proceeding with regard to the level of specificity they provide to the recipients. *See, e.g., FTC v. O'Connell Assocs., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (resolution “[t]o determine whether unnamed consumer reporting agencies . . . may be engaged in acts or practices in violation of Section 5”); *FTC v. Nat’l Claims Serv.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (resolution to investigate unnamed firms that sell “business opportunities . . . to consumers [and] . . . are engaged in unfair or deceptive acts or practices in violation of . . . Section 5”).

As for respondents’ further contention that the Commission may not inquire into their practices relating to data security, the Commission discredited this assertion in ruling on the petitions to quash. Pet. Exh. 6, at 10-13. Most importantly, there is no legal authority suggesting that HIPAA repealed the FTC’s jurisdiction to investigate the security of sensitive health information. To the contrary, the Preamble to the HHS Privacy Rule anticipates that HIPAA-covered entities are “also subject to

other federal statutes and regulations.” 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000).¹¹ Consistently, the two agencies have coordinated other information security actions involving sensitive health information covered by HIPAA.¹²

As the Commission explained, “courts rarely hold that one federal statute impliedly repeals another because ‘when two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective.’” Pet. Exh. 6, at 12 (quoting *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976)). Consistent with these principles, courts have consistently rejected challenges to FTC law enforcement actions in instances where the Commission sought to exercise authority shared with other federal enforcement agencies. *See, e.g., FTC v. Cement Inst.*, 333 U.S. 683, 694 (1948) (FTC and DOJ have overlapping jurisdiction to bring civil actions for unfair methods of competition); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986) (FTC and FDA share jurisdiction to regulate advertising for over-the-counter

¹¹ Additionally, the Preamble contains a section entitled “Implied Repeal Analysis,” which is silent on any ostensible repeal of the FTC Act. 65 Fed. Reg. At 82,481-87.

¹² *See In re CVS Caremark Corp.*, FTC File. No. 0723119 (February 18, 2009), available at <http://www.ftc.gov/opa/2009/02/cvs.shtm> (settlement agreements resolving coordinated FTC-HHS information security investigations); *In re Rite Aid Corp.*, FTC File No. 0723121 (July 27, 2010), available at <http://www.ftc.gov/opa/2010/07/riteaid.shtm> (same).

drugs). In short, “this is an era of overlapping agency jurisdiction under different statutory mandates.” *Texaco*, 555 F.2d at 881. While HHS has a statutory mandate to provide consumers with access to their health information and to prevent inappropriate use of that information, *see* 65 Fed. Reg. at 82,463, the FTC has a broader, but complementary, mandate – to prevent deceptive or unfair practices – as well as complementary remedies. *See* 15 U.S.C. § 45(a).

In any event, this CID enforcement proceeding is “not the proper forum in which to litigate the question of coverage under a particular statute. . . . The initial determination of the coverage question is left to the administrative agency seeking enforcement.” *Kloster Cruise*, 939 F.2d at 922 (quoting *EEOC v. Peat, Marwick, Mitchell & Co.*, 775 F.2d 928, 930 (8th Cir. 1985)). The Commission need only make a “plausible argument” in support of its jurisdiction. *Kloster Cruise*, 939 F.2d at 922 (internal citation omitted).¹³ The FTC is entitled to investigate the nature and scope of LabMD’s security practices without inviting a premature attack on statutory coverage. Respondents’ arguments to the contrary would “not only place the cart before the horse, but [] substitute a different driver for the one appointed by

¹³ *See also New Orleans Pub. Serv., Inc. v. Brown*, 507 F.2d 160, 165 (5th Cir. 1975); *FTC v. Gibson*, 460 F.2d 605, 608 (5th Cir. 1972); *United States v. Feaster*, 376 F.2d 147, 148 (5th Cir. 1967).

Congress.” *Kloster Cruise*, 939 F.2d at 924 (quoting *EEOC v. Chrysler Corp.*, 567 F.2d 754, 755 (8th Cir. 1977)).

C. The CIDs Seek Information That is Reasonably Relevant to the Commission’s Investigation

The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudication. In an investigation, the Commission is not limited to seeking information that is necessary to prove specific charges. It merely seeks to learn whether there is reason to believe that the law is being violated and, if so, whether the issuance of a complaint would be in the public interest. *See Texaco*, 555 F.2d at 872; *see also Florida Azalea*, 19 F.3d 622-23 (an agency “can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not”) (quoting *Morton Salt*, 338 U.S. at 642-43). The CIDs’ required testimony and information, therefore, need only be relevant to the investigation – the boundary of which may be defined by the agency quite generally. *See Carter*, 636 F.2d at 787-88; *Texaco*, 555 F.2d at 874 & n.26.

In the present investigation, the Commission is seeking to determine whether LabMD and Mr. Daugherty have engaged in deceptive or unfair practices in connection with their patients’ privacy and data security. The revelation that LabMD’s 1,718 File (containing the confidential information of over 9,000 patients)

was available for public download on a P2P network provides grounds to inquire whether its security practices were unreasonable and therefore could be unfair or deceptive. The Commission, however, has been stymied in its efforts to ask LabMD and Mr. Daugherty about LabMD's data security practices, such as informal practices and procedures, and about the responsibilities of Mr. Daugherty, LabMD's president and owner. Pet. Exh. 1 ¶¶ 7-8, 12-13. Such questions are "reasonably relevant" to an investigation into "unfair or deceptive acts or practices [involving] consumer privacy and/or data security." See Pet. Exh. 2, 3; *Florida Azalea*, 19 F.3d at 624.

As the Commission explained when rejecting the petitions to quash, it is premature to consider the underlying merits of LabMD's potential liability under the FTC Act until the CIDs have been enforced and the investigation is complete. See, pp. 8-9, *supra*. "A party under investigation may not contest the discovery and production of evidence in the same manner he may contest the use of that evidence in an adjudication by proper objection, by the introduction of other evidence, and other safeguards traditional to an adversary proceeding under our system." *Genuine Parts Co. v. FTC*, 445 F.2d 1382, 1388 (5th Cir. 1971). The Commission is entitled to investigate the circumstances that led the 1,718 File to become available for public download on a P2P network, and whether LabMD engaged in unfair or deceptive practices by failing to take reasonable steps to safeguard the File, regardless of

whether the File was first discovered by a party with proper access.¹⁴ Any assertion that “the Commission, in its investigation, must not ask any questions to which it does not already know the answers, has about it the aura of another, and bygone, legal era.” *New Orleans Pub. Serv., Inc. v. Brown*, 507 F.2d 160, 164 (5th Cir. 1975).

D. The CIDs Are Not Unreasonably Broad or Burdensome

As the Commission concluded in denying petitions to quash, respondents cannot demonstrate that complying with the CIDs is unduly burdensome. *See FTC v. Jim Walter Corp.*, 651 F.2d 251, 258 (5th Cir. Unit A July 1981), *abrogated on other grounds by Ins. Corp. of Ireland v. Compagnie de Bauxites de Guinee*, 456 U.S. 694, 702-03 (1982). It is well established that “a subpoena is not unreasonably burdensome unless ‘compliance threatens to unduly disrupt or seriously hinder normal operations of a business.’” *Jim Walter*, 651 F.2d at 258 (quoting *Texaco*, 555 F.2d at 882). Respondents do not satisfy this standard because the CIDs principally seek oral testimony and, as the Commission noted, they do not require a large-scale or time-

¹⁴ Even if Tiversa located and downloaded the 1,718 File from a P2P network, LabMD “had no reasonable expectation of privacy” in files its computers made accessible to a P2P network. *See United States v. Gabel*, No. 10-60168, 2010 WL 3927697, at *7 (S.D. Fla. Sep. 16, 2010). LabMD “was, essentially, sharing them with the entire world. *Anyone* with internet access could have easily downloaded [P2P] client software, logged on to the network and downloaded [the] files.” *Id.* (emphasis in original).

consuming document production. Pet. Ex. 6, at 7-8. Such a limited obligation on respondents' part does not constitute "undue burden" under any reasonable sense of the term.

CONCLUSION

For all the foregoing reasons, this Court should grant the Commission's petition and enter its own order requiring LabMD and Mr. Daugherty to comply in full with the December 21, 2011 civil investigative demands within 10 days of the Court's order, or at such later date as may be established by the Commission.

Respectfully submitted,

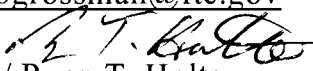
WILLARD K. TOM
General Counsel

JOHN F. DALY
Deputy General Counsel for Litigation

LESLIE RICE MELMAN
Assistant General Counsel for Litigation

BURKE W. KAPPLER
BRADLEY D. GROSSMAN
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
Telephone: (202) 326-2043 (Kappler)
Telephone: (202) 326-2994 (Grossman)
Fax: (202) 326-2477
Email: bkappler@ftc.gov
Email: bgrossman@ftc.gov

LOCAL COUNSEL:


s/ Ryan T. Holte

RYAN T. HOLTE
Georgia Bar No. 156327
CINDY A. LIEBES
Georgia Bar No. 451976
Federal Trade Commission
Suite 1500
225 Peachtree Street, NE
Atlanta, GA 30303
Telephone: (404) 656-1360 (Holte)
Telephone: (404) 656-1359 (Liebes)
Fax: (404) 656-1379
Email: rholt@ftc.gov
Email: cliebes@ftc.gov

Dated: August 29, 2012

Certification of Font and Margins

Pursuant LR 7.1D, I hereby certify that the foregoing document was prepared using 14 point Times New Roman font and complies with the margin and type requirements of this Court.



s/ Ryan T. Holte

Ryan T. Holte

JS44 (Rev. 04/12 NDGA)

CIVIL COVER SHEET

12-CV-3005

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

DEFENDANT(S)

LabMD, Inc., and Michael J. Daugherty
2030 Powers Ferry Road
Building 500, Suite 520
Atlanta, Georgia 30339

WSD

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF _____
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Cobb
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Ryan T. Holte and Cindy A. Liebes (Local Counsel), Federal Trade Commission, 225 Peachtree Street, NE, Suite 1500, Atlanta, GA 30303 (404) 656-1360, rholte@ftc.gov
Burke Kappler and Bradley Grossman, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, (202) 326-2043, bkappler@ftc.gov

ATTORNEYS (IF KNOWN)

Stephen F. Fusco, LabMD, Inc., 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339, (678) 443-2343, sfusco@labmd.org

II. BASIS OF JURISDICTION
(PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF
- 2 U.S. GOVERNMENT DEFENDANT
- 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES
(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

- | PLF | DEF | PLF | DEF |
|----------------------------|----------------------------|----------------------------|----------------------------|
| <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |
- 1 CITIZEN OF THIS STATE
2 CITIZEN OF ANOTHER STATE
3 CITIZEN OR SUBJECT OF A FOREIGN COUNTRY
4 INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
5 INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
6 FOREIGN NATION

IV. ORIGIN (PLACE AN "X" IN ONE BOX ONLY)

- 1 ORIGINAL PROCEEDING
- 2 REMOVED FROM STATE COURT
- 3 REMANDED FROM APPELLATE COURT
- 4 REINSTATED OR REOPENED
- 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- 6 MULTIDISTRICT LITIGATION
- 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Petition to enforce civil investigative demands issued by the Federal Trade Commission pursuant to 15 U.S.C. §§ 56 and 57b-1

(IF COMPLEX, CHECK REASON BELOW)

- 1. Unusually large number of parties.
- 2. Unusually large number of claims or defenses.
- 3. Factual issues are exceptionally complex
- 4. Greater than normal volume of evidence.
- 5. Extended discovery period is needed.
- 6. Problems locating or preserving evidence
- 7. Pending parallel investigations or actions by government.
- 8. Multiple use of experts.
- 9. Need for discovery outside United States boundaries.
- 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

| | | | |
|-----------------|--------------------------------|----------------------|------------------------|
| RECEIPT # _____ | AMOUNT \$ _____ | APPLYING IFP _____ | MAG. JUDGE (IFP) _____ |
| JUDGE _____ | MAG. JUDGE _____ (Referral) | NATURE OF SUIT _____ | CAUSE OF ACTION _____ |

WSD 890 15:0015

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK

- 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK

- 110 INSURANCE
- 120 MARINE
- 130 MILLER ACT
- 140 NEGOTIABLE INSTRUMENT
- 151 MEDICARE ACT
- 160 STOCKHOLDERS' SUITS
- 190 OTHER CONTRACT
- 195 CONTRACT PRODUCT LIABILITY
- 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 210 LAND CONDEMNATION
- 220 FORECLOSURE
- 230 RENT LEASE & EJECTMENT
- 240 TORTS TO LAND
- 245 TORT PRODUCT LIABILITY
- 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK

- 310 AIRPLANE
- 315 AIRPLANE PRODUCT LIABILITY
- 320 ASSAULT, LIBEL & SLANDER
- 330 FEDERAL EMPLOYERS' LIABILITY
- 340 MARINE
- 345 MARINE PRODUCT LIABILITY
- 350 MOTOR VEHICLE
- 355 MOTOR VEHICLE PRODUCT LIABILITY
- 360 OTHER PERSONAL INJURY
- 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- 365 PERSONAL INJURY - PRODUCT LIABILITY
- 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 370 OTHER FRAUD
- 371 TRUTH IN LENDING
- 380 OTHER PERSONAL PROPERTY DAMAGE
- 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- 422 APPEAL 28 USC 158
- 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK

- 441 VOTING
- 442 EMPLOYMENT
- 443 HOUSING/ ACCOMMODATIONS
- 444 WELFARE
- 440 OTHER CIVIL RIGHTS
- 445 AMERICANS with DISABILITIES - Employment
- 446 AMERICANS with DISABILITIES - Other
- 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- 462 NATURALIZATION APPLICATION
- 463 HABEAS CORPUS- Alien Detainee
- 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK

- 510 MOTIONS TO VACATE SENTENCE
- 530 HABEAS CORPUS
- 535 HABEAS CORPUS DEATH PENALTY
- 540 MANDAMUS & OTHER
- 550 CIVIL RIGHTS - Filed Pro se
- 555 PRISON CONDITION(S) - Filed Pro se
- 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK

- 550 CIVIL RIGHTS - Filed by Counsel
- 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK

- 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK

- 710 FAIR LABOR STANDARDS ACT
- 720 LABOR/MGMT. RELATIONS
- 740 RAILWAY LABOR ACT
- 751 FAMILY and MEDICAL LEAVE ACT
- 790 OTHER LABOR LITIGATION
- 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- 820 COPYRIGHTS
- 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- 830 PATENT

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK

- 861 HIA (1395(f))
- 862 BLACK LUNG (923)
- 863 DIWC (405(g))
- 863 DIWW (405(g))
- 864 SSDI TITLE XVI
- 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK

- 870 TAXES (U.S. Plaintiff or Defendant)
- 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK

- 375 FALSE CLAIMS ACT
- 400 STATE REAPPORTIONMENT
- 430 BANKS AND BANKING
- 450 COMMERCE/ICC RATES/ETC.
- 460 DEPORTATION
- 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- 480 CONSUMER CREDIT
- 490 CABLE/SATELLITE TV
- 891 AGRICULTURAL ACTS
- 893 ENVIRONMENTAL MATTERS
- 895 FREEDOM OF INFORMATION ACT
- 950 CONSTITUTIONALITY OF STATE STATUTES
- 890 OTHER STATUTORY ACTIONS
- 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK

- 410 ANTITRUST
- 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK

- 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND \$ _____
 JURY DEMAND YES NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE _____ DOCKET NO. _____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- 1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.
- 5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.
- 6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):
- 7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. _____, WHICH WAS DISMISSED. This case IS IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.

/s/ Ryan T. Holte 
 SIGNATURE OF ATTORNEY OF RECORD

8/29/2012 8/29/12
 DATE