ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051

http://oversight.house.gov

December 1, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Ms. Ramirez:

The Committee on Oversight and Government Reform has been investigating the activities of Tiversa, Inc., a Pittsburgh-based company that purportedly provides peer-to-peer intelligence services. The Federal Trade Commission has relied on Tiversa as a source of information in its enforcement action against LabMD, Inc., a Georgia-based medical testing laboratory. The Committee has obtained documents and information indicating Tiversa failed to provide full and complete information about work it performed regarding the inadvertent leak of LabMD data on peer-to-peer computer networks. In fact, it appears that, in responding to an FTC subpoena issued on September 30, 2013, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

Despite a broad subpoena request, Tiversa provided only summary information to the FTC about its knowledge of the source and spread of the LabMD file.

Initially, Tiversa, through an entity known as the Privacy Institute, provided the FTC with information about peer-to-peer data leaks at nearly 100 companies, including LabMD.[1] Tiversa created the Privacy Institute for the specific purpose of providing information to the FTC. Despite Tiversa's claims that it is a trusted government partner, it did not want to disclose that it provided information to the FTC.[2]

After the FTC filed a complaint against LabMD, the agency served Tiversa with a subpoena for documents related to the matter. Among other categories of documents, the subpoena requested "all documents related to LabMD."[3] In a transcribed interview, Alain Sheer,

[1] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback, Chief Executive Officer, Tiversa, Inc., Transcript at 42 (June 5, 2014) [hereinafter Boback Tr.].
[2] *See* Tiversa, Industry Outlook, Government/Law Enforcement, *available at* http://tiversa.com/explore/industry/gov (last visited Nov. 21, 2014); Boback Tr. at 42-43.
[3] Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC Subpoena].

an attorney with the FTC's Bureau of Consumer Protection, told the Committee that the FTC did not narrow the subpoena for Tiversa. Sheer stated:

> Q This is the specifications requested of Tiversa. No. 4 requests all documents related to LabMD. Do you know if Tiversa produced all documents related to LabMD?
>
> A I am not sure what your question is.
>
> Q Let me ask it a different way. Was the subpoena narrowed in any way for Tiversa?
>
> A Not that I am aware of.[4]

In total, Tiversa produced 8,669 pages of documents in response to the FTC's subpoena. Notably, the production contained five copies of the 1,718-page LabMD Insurance Aging file that Tiversa claimed to have found on peer-to-peer networks and only 79 pages of other materials, none of which materially substantiated Tiversa's claims about the discovery of the file.

The information Tiversa gave the FTC included the IP address from which Tiversa CEO Robert Boback has claimed the company first downloaded the LabMD file, as well as other IP addresses that Tiversa claims also downloaded the file. The origin of the IP address from which Tiversa first downloaded the LabMD file was in dispute in other litigation between LabMD and Tiversa. On numerous occasions, including before the FTC, Boback maintained that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. Boback stated:

> Q What is the significance of the IP address, which is 68.107.85.250?
>
> A That would be the IP address that we downloaded the file from, I believe.
>
> Q Going back to CX 21. Is this the initial disclosure source?
>
> A If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.
>
> Q When did Tiversa download [the LabMD file]?
>
> A I believe it was in February of 2008.[5]

---

[4] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer, Fed. Trade Comm'n, Transcript at 147 (Oct. 9, 2014).

[5] In the matter of LabMD, Inc., Deposition of Robert J. Boback, CEO, Tiversa, transcript at 24-25 (Nov. 21, 2013) [hereinafter Boback Nov. 2013 FTC Tr.].

Boback also testified that Tiversa performed an investigation into the LabMD file at the request of a client.[6] In the course of this investigation, Tiversa concluded that an IP address in Atlanta, Georgia, where LabMD was headquartered, was the initial disclosure source of the document. Boback stated:

> Q There is an IP address on the right-hand side, it is 64.190.82.42. What is that?
>
> A That, if I recall, is an IP address that resolves to Atlanta, Georgia.
>
> Q Is that the initial disclosure source?
>
> A We believe that it is the initial disclosure source, yes.
>
> Q And what is that based on?
>
> A The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.
>
> * * *
>
> Q So, I think you are telling me that chronologically this was the first other location for that file in juxtaposition of when you found the file at 68.107.85.250?
>
> A We know that the file in early February, prior to this February 25 date, was downloaded from the 68.107.85.250. Upon a search to determine other locations of the file across the network, it appears that on 2/25/2008 we had a hash match search at 64.190.82.42, which resolved to Atlanta, which led us to believe that without further investigation, that this is most likely the initial disclosing source.
>
> Q What other information do you have about 64.190.82.42?
>
> A I have no other information. I never downloaded the file from them. They only responded to the hash match.[7]

Boback's testimony before the FTC in November 2013 made clear that Tiversa first downloaded the LabMD file from an IP address in San Diego, California, in February 2008, that it only identified LabMD as the disclosing source after performing an investigation requested by a client, and that it never downloaded the file from LabMD.

---

[6] Boback Nov. 2013 FTC Tr. at 72-73 ("In 2008, when working for another client, we were attempting to identify the original disclosure source of the file that we discovered from 1 the San Diego IP address.").
[7] Boback Nov. 2013 FTC Tr. at 41.

Tiversa withheld responsive documents from the FTC, despite the issuance of the September 2013 subpoena. These documents contradict the account Boback provided to the FTC.

On June 3, 2014, the Committee issued a subpoena to Tiversa requesting, among other information, "[a]ll documents and communications referring or relating to LabMD, Inc."[8] This request was very similar to the FTC's request for "all documents related to LabMD."[9] Despite nearly identical requests from the FTC and the Committee to Tiversa, Tiversa produced numerous documents to the Committee that it does not appear to have produced to the FTC. Information contained in the documents Tiversa apparently withheld contradicts documents and testimony Tiversa did provide to the FTC.

An internal Tiversa document entitled "Incident Record Form," dated April 18, 2008, appears to be the earliest reference to the LabMD file in Tiversa's production to the Committee.[10] This document states that on April 18, 2008, Tiversa detected a file "disclosed by what appears to be a potential provider of services for CIGNA."[11] The Incident Record described the document as a "single Portable Document Format (PDF) that contain[ed] sensitive data on over 8,300 patients," and explained that "[a]fter reviewing the IP address, resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source."[12] The name of the file was "insuranceaging_6.05.071.pdf," which is the same name as the file in question in the FTC proceeding. According to the Incident Record, the IP address disclosing the file was 64.190.82.42—later confirmed to be a LabMD IP address.[13] Upon learning about the file, CIGNA, a Tiversa client, "asked Tiversa to perform Forensic Investigation activities" on the insurance aging file to determine the extent of proliferation of the file over peer-to-peer networks.[14]

An August 2008 Forensic Investigation Report provided the analysis CIGNA requested. This report identified IP address 64.190.82.42—the Atlanta IP address—as proliferation point zero, and the "original source" of the Incident Record Form.[15] A spread analysis included in the August 2008 forensic report stated that the file had been "observed by Tiversa at additional IP addresses" but made clear that Tiversa had not downloaded the file from either additional source because of "network constraint and/or user behavior."[16] Thus, according to this report, Tiversa had only downloaded the LabMD file from one source in Atlanta, Georgia by August 2008. This contradicts Boback's testimony that Tiversa first downloaded the LabMD file from an IP address

---

[8] H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014).
[9] Tiversa FTC Subpoena.
[10] Tiversa Incident Record Form, ID # CIG00081 (Apr. 18, 2008).
[11] *Id.*
[12] *Id.* (emphasis added).
[13] *Id.*
[14] Tiversa, Forensic Investigation Report for Ticket #CIG00081 (Aug. 12, 2008). This letter uses the phrase "forensic report" to describe this and a second report created by Tiversa about the LabMD file because that is the title used by Tiversa. It is not clear what, if any, forensic capabilities Tiversa possesses.
[15] *Id.*
[16] *Id.*

in San Diego, California. If Tiversa had in fact downloaded the LabMD file from a San Diego IP address in February 2008, then that fact should be included in this 2008 forensic report. It is not.

One of the two additional IP addresses is located in San Diego, California. It is a different IP address, however, than the one from which Tiversa claims to have originally downloaded the file.[17] Further, Tiversa did not observe that this San Diego IP address possessed the LabMD file until August 5, 2008.[18] Thus, according to this report, Tiversa did not observe any San Diego IP address in possession of the LabMD file until August 2008. Again, the report stands in stark contrast to Boback's testimony that Tiversa first downloaded the LabMD file from a different San Diego IP address in February 2008.

In addition, both the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report stated that the LabMD file was "detected being disclosed" in April 2008. Neither report indicated that Tiversa first downloaded the file from the San Diego IP address—an IP address not listed on either report—on February 5, 2008. Boback's deposition testimony and a cursory four-line document marked as exhibit CX-19 seem to be the only evidence that Tiversa first downloaded the LabMD file from a San Diego IP address in February 2008.

These documents contradict the information Tiversa provided to the FTC about the source and spread of the LabMD file. If Tiversa had, in fact, downloaded the LabMD file from the San Diego IP address and not from the Georgia IP address, then these reports should indicate as such. Instead, the San Diego IP address is nowhere to be found, and the Georgia IP address appears as the initial disclosing source on both reports.

Tiversa also produced an e-mail indicating that it originally downloaded the LabMD file from Georgia – and not from San Diego as it has steadfastly maintained to the FTC and this Committee. On September 5, 2013, Boback e-mailed Dan Kopchak and Molly Trunzo, both Tiversa employees, with a detailed summary of Tiversa's involvement with LabMD. Why Boback drafted the e-mail is unclear. He wrote, "[i]n 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."[19]

As noted above, according to Alain Sheer, a senior FTC attorney assigned to the LabMD matter, the FTC did not narrow the September 2013 subpoena requiring Tiversa to produce, among other documents, "all documents related to LabMD."[20] Tiversa withheld these relevant

---

[17] The IP address reported on the August 2008 forensic report that resolves to San Diego, California is 68.8.250.203. Boback testified, however, that Tiversa first downloaded the LabMD file from IP address 68.107.85.250 on February 5, 2008. Tiversa concluded in the report that the second IP address on which it observed the file was "most likely an IP shift from the original disclosing source."

[18] *Id.*

[19] E-mail from Robert Boback, CEO, Tiversa, to Dan Kopchak & Molly Trunzo (Sept. 5, 2013) (emphasis added) [TIVERSA-OGR-0028866-67].

[20] Tiversa FTC Subpoena.

documents about its discovery and early forensic analysis of the LabMD file from the FTC. These documents directly contradict testimony that Boback provided to the FTC, and call Tiversa's credibility into question. Boback has not adequately explained why his company withheld documents, and why his testimony is not consistent with reports Tiversa created at the time it discovered the LabMD file.

It is unlikely that the LabMD file analyzed in the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report is different from the so-called "1718 file" at issue in the FTC proceeding, particularly given Boback's testimony to the FTC about how Tiversa's system names files.[21] If, however, the earlier reports do refer to a different file, then Tiversa neglected to inform the FTC of a second, similarly sized leak of LabMD patient information.

Tiversa's June 2014 forensic report is the only report provided to this Committee that substantiates Boback's claims.

Tiversa produced to the Committee a forensic report on the LabMD file that it created in June 2014. Tiversa created this report and others related to testimony previously provided to the Committee after the investigation began. While outside the scope of the FTC's subpoena due to the date of the document, this is the only report supporting Tiversa's claim that it first downloaded the file from the San Diego IP address. This report contradicts information Tiversa provided to CIGNA in the April 2008 Incident Record Form and August 2008 Forensic Investigative Report—documents created much closer to when Tiversa purportedly discovered the LabMD document on a peer-to-peer network. The fact that Tiversa created the only forensic report substantiating its version of events after the Committee began its investigation raises serious questions.

This most recent report states that Tiversa's systems first detected the file on February 5, 2008, from a San Diego IP address (68.107.85.250) not included in either of the 2008 documents. According to the spread analysis, this San Diego IP shared the file from February 5, 2008, until September 20, 2011. Yet, despite allegedly being downloaded before both the April or August 2008 reports, neither 2008 document mentions that Tiversa downloaded this document.

The June 2014 report also states that the LabMD IP address (64.190.82.42) shared the file between March 7, 2007, and February 25, 2008. Thus, according to this report, by the time Tiversa submitted an Incident Record Form to CIGNA in April 2008, the LabMD IP address was no longer sharing the file. Furthermore, the report does not describe why Tiversa's system did not download the file from the Georgia IP address, even though the technology should have downloaded a file that hit on a search term, in this case "CIGNA," each time a different computer shared the document. The June 2014 report includes no reference to the other San Diego IP address discussed in the August 2008 forensic report as being in possession of the LabMD file.

---

[21] Boback Nov. 2013 FTC Tr. at 40-41 (describing that a file's "hash" or title identifies "exactly what that file is." The title of the LabMD document described in the April and August 2008 documents is the same as the title of the document in the FTC proceeding).

Tiversa did not make a full and complete production of documents to this Committee. It is likely that Tiversa withheld additional documents from both this Committee and the FTC.

On October 14, 2014, Tiversa submitted a Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity.[22] Chief Administrative Law Judge D. Michael Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose."[23] Tiversa included two e-mails from 2012 as exhibits to the Notice of Information. According to Tiversa, these e-mails demonstrate that Wallace could not have fabricated the IP addresses in question in October 2013, because he previously included many of them in e-mails to himself and Boback a year prior.[24]

Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission in the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. In its Notice of Information, Tiversa did not explain how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information and do not explain what exactly Wallace conveyed to Boback in November 2012 or why he conveyed it.

If Boback did in fact receive this information in November 2012, his June 2013 deposition testimony is questionable. It is surprising that Tiversa would have supplied inaccurate information to the FTC when Boback himself apparently received different information just months prior. Tiversa should have located and produced these e-mails pursuant to the September 2013 subpoena, and it should have been available for Boback's June 2013 deposition.

Tiversa's failure to produce numerous relevant documents to the Commission demonstrates a lack of good faith in the manner in which the company has responded to subpoenas from both the FTC and the Committee. It also calls into question Tiversa's credibility as a source of information for the FTC. The fact remains that withheld documents contemporaneous with Tiversa's discovery of the LabMD file directly contradict the testimony and documents Tiversa did provide. In the Committee's estimation, the FTC should no longer consider Tiversa to be a cooperating witness. Should the FTC request any further documents from Tiversa, the Commission should take all possible steps to ensure that Tiversa does not withhold additional documents relevant to the proceeding.

---

[22] Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request For Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014), http://www.ftc.gov/system/files/documents/cases/572572.pdf [hereinafter Notice of Information].

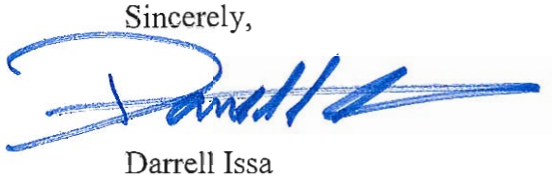
[23] *LabMD Case: FTC gets green light to grant former Tiversa employee immunity in data security case*, PHIprivacy.net, Nov. 19, 2014, http://www.phiprivacy.net/labmd-case-ftc-gets-green-light-to-grant-former-tiversa-employee-immunity-in-data-security-case/.

[24] Notice of Information at 4.

I have enclosed the documents discussed herein with this letter, so that your staff may examine them. All documents are provided in the same form in which Tiversa produced them to the Committee.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X. If you have any questions, please contact the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,



Darrell Issa
Chairman

Enclosures

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

Ms. Kelly Tshibaka, Acting Inspector General, U.S. Federal Trade Commission

Ms. Laura Riposo VanDruff, Complaint Counsel, U.S. Federal Trade Commission

TIVERSA

INVESTIGATION REQUEST FORM

Section 1 Customer Information	
Organization Name	CIGNA
Contact Name	Sean Ryan
Contact Phone Number	(860) 226-7107
Contact Email Address	sean.ryan@cigna.com

Section 2 Incident Information	
Tiversa Incident Number	CIG00081
Date of Incident	4/18/2008

Section 3 Requested Forensic Services	
File Disclosure Investigation	**Search Investigation**
☐ 1. Disclosure Source Identification ☐ 2. Disclosure Source Geo-location ☐ 3. Identify Additional Disclosure Source Files ☐ 4. File Proliferation Assessment ☐ 5. Proliferation Point Identification ☐ 6. Proliferation Point Geo-location ☐ 7. Proliferation Point Associated Files	☐ 12. Review Stored Searches For File Targeting ☐ 13. Track Searches for Specific File or Term
Persons of Interest (PoI)	**Miscellaneous**
☐ 8. Identify Persons of Interest ☐ 9. Track Specific Behavior of Persons of Interest ☐ 10. Identify Files Associated with Persons of Interest ☐ 11. Track Persons of Interest Download Behavior	☐ 14. Prosecution Support (Complete Section 4) ☐ 15. Other (Complete Section 4)

Section 4 Specific Information Related to Request

TIVERSA

INCIDENT RECORD FORM

Section 1 Customer Information	
Organization Name	CIGNA
Contact Name	Sean Ryan
Contact Phone Number	(860) 226-7107
Contact Email Address	sean.ryan@cigna.com

Section 2 Incident Information	
Tiversa Incident Number	CIG00081
Related Tiversa Incident Numbers	None
Date of Incident	4/18/2008
Severity	Urgent

Section 3 Disclosure Information	
IP Address	64.190.82.42
Disclosure Type	Partner / Provider
Summary Disclosure Name/ID	LAB MD
Filenames	[64.190.82.42]insuranceaging_6.05.071.pdf

Section 4 Incident Summary

On 4/18/2008, 1 file was detected being disclosed by what appears to be a potential provider of services for CIGNA.

The information appears to be a single Portable Document Format (PDF) file that contains sensitive data on over 8,300 patients. Some of the information includes: Patients Full Name, SSN, DOB, Insurance Policy Numbers, Patient Diagnostic Codes, and other information. Of the 8,342 patient records, at least 113 appear to be listed as insured by CIGNA.

After reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.

Section 5 Additional Questions That Tiversa Can Address
More information can be gathered related to this disclosure by leveraging Tiversa's P2P File Sharing Forensic Investigation Services. If requested, please fill out the Investigation Request form located below and submit to your Account Manager.
Who is the individual disclosing the information?
Select investigation services #1 and #3
What else is this individual sharing or disclosing?
Select investigation service #3
Where is this individual located in the world?
Select investigation service #2
Did the files spread to other users of the network?
Select investigation services #4

TIVERSA™

Forensic Investigation Report for Ticket #CIG00081

August 12, 2008

CONFIDENTIAL

1. Introduction

Tiversa monitors peer-to-peer file sharing networks (P2P) for CIGNA 24/7/365 to identify disclosed sensitive or confidential CIGNA-related information and to record P2P users searching for this information. For each file disclosure, Tiversa provides a disclosure ticket to CIGNA. Each ticket includes the name of the file(s) disclosed, IP on which the files were obtained, the likely source of the disclosure, and copies of the disclosed files. In some cases, more information is required in order to decide what actions to take or to determine if remedial actions have worked. In these instances, Forensic Investigation Services are required.

This Forensic Investigation Report (FIR) summarizes the results and suggested actions of Tiversa's Forensic Investigation Services for Ticket CIG00081, as requested by CIGNA.

1.1 Ticket CIG00081 Summary

The specifics of this ticket as reported were as follows:

- Date Submitted: 4/18/2008
- Disclosing IP Location: 64.190.82.42
- Number of Files Disclosed: 1 CIGNA file (19 total files)
- Probable Disclosure Source: Partner/Provider
- Probable Disclosure Name/ID: Lab MD
- Severity: Urgent

Ticket Write-up Copy:
On 4/18/2008, 1 file was detected being disclosed by what appears to be a potential provider of services for CIGNA.

The information appears to be a single Portable Document Format (PDF) file that contains sensitive data on over 8,300 patients. Some of the information includes: Patients Full Name, SSN, DOB, Insurance Policy Numbers, Patient Diagnostic Codes, and other information. Of the 8,342 patient records, at least 113 appear to be listed as insured by CIGNA.

After reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.

CIGNA asked Tiversa to perform Forensic Investigation activities related to the above ticket in order to ascertain if any of the disclosed files have proliferated across the P2P.

2. Investigation Findings

2.1 File Proliferation Analysis

The CIGNA-related file identified in Ticket #81, as well as some of the files not related to CIGNA, have been observed by Tiversa at additional IP addresses on the P2P. However, network constraints and/or user behavior prevented Tiversa from downloading the files from these additional sources. Most likely, the user logged off the P2P prior to or while Tiversa was attempting to acquire the files.

Regardless, information regarding these new observations is included in Figure 2-1-1 immediately below.

Figure 2-1-1:
File Proliferation Details

Proliferation Point	File Title	IP Address	Date Observed	IP Geo-Location	ISP	Source
0	insuranceaging_6.05.071.pdf	64.190.82.42	4/18/08	Atlanta, GA	Cypress Communications	Original Source from Ticket #81
1	insuranceaging_6.05.071.pdf	64.190.79.36	8/1/08	Oakwood, GA	Cypress Communications	Probably an IP shift of original source
2	insuranceaging_6.05.071.pdf	68.8.250.203	8/5/08	San Diego, CA	Cox Communications	Unknown (based on other files observed, possible Information Concentrator)

Based on the other files available at the new IP addresses, Proliferation Point #1 (from Figure 2-1-1 above) is most likely an IP shift from the original disclosing source identified in Ticket #81. However, the other files present at Proliferation Point #2 suggest that this source could be an Information Concentrator. Because Tiversa analysts were only able to visually observe these new sources, rather than actually download files, further data collection and analysis may be required for full source identification of the proliferation points.

2.2 Additional Data Collection/ Analysis

Tiversa is currently attempting to re-acquire these sources and download any relevant files from them.

3. Conclusions/ Suggested Actions

It appears evident that the files from Ticket #81 have proliferated across the P2P and are available from additional IP addresses. However, clear identification of these new sources is not conclusive at this time. Tiversa will update this report as new information becomes available.

In the meantime, CIGNA and/or LabMD investigations of the data currently available could be executed. If additional data from Tiversa is required, it can be provided -- for instance, a full listing of files disclosed from the original source (even if those files are not related to CIGNA) can be made available.

TIVERSA

2000 Corporate Drive, Suite 300
Wexford, Pennsylvania 15090

724 940-9030
724 940-9033

www.tiversa.com

From: Robert Boback <rboback@tiversa.com>
Sent: Thursday, September 5, 2013 3:20 PM
To: Dan Kopchak <dkopchak@tiversa.com>; Molly Trunzo <mtrunzo@tiversa.com>
Subject: Tiversa

I wanted to provide updated information regarding the question of litigation involving Tiversa. During our call, I discussed litigation in which Tiversa is a pla against our former patent firm. That is still ongoing. Earlier in 2013, Tiversa was also engaged in a separate litigation with a company called LabMD, which is base in Georgia. Tiversa, Dartmouth College and Professor Eric Johnson (Tuck Business School) was sued by LabMD by its CEO, Michael Daugherty as he alleged that Tiversa "hacked" his company in an effort to get a file containing nearly 9,000 patient's SSNs and medical information and provided the information to Dartmouth and Eric Johnson for a DHS-funded research project. Mr. Daugherty has little to no understanding of P2P or Information security which is what caused him to think that he was "hacked" and which resulted in his widespread government conspiracy theory that followed. He also suggested in the litigation that because he woul not do business with Tiversa to remediate the problem, that Tiversa "kicked the file over to the feds [FTC]" (and Dartmouth) and the FTC sent him a questionnaire about the breach, which caused him "great harm" due to the widespread "government shakedown of small business." He claimed that Tiversa was attempting to extort money from him to "answer his questions" as a part of the larger conspiracy. The reason that I did not mention this during our discussion is that the case was dismissed due to jurisdiction (his real estate attorney friend filed it in Georgia). He subsequently appealed two times, and lost both, the final of which was ruled on in February 2013. As an interesting sidebar to this story, Mr. Daugherty began writing a book about the government overreach and his great conspiracy theory o the government war on small business. When our attorneys learned of what was coming in the book (from his blog postings about the book), we quickly served his counsel with a C&D as his "true story" was full of inaccurate statements about me and Tiversa. Unfortunately, Mr. Daugherty sees himself as "Batman" (no joke) and he chose to continue on with his book and starting scheduling speaking engagements where he would discuss his "true story" about how the government is out to "get" small business and that the FTC and Tiversa (and presumably Dartmouth) are the ring leaders. His book, "Devil inside the Beltway" is to be released later this month. While I do not expect this book to be on the NY Times best seller list, I cannot sit idly by and allow such a gross distortion of the facts and mischaracterization of Tiversa, and me, in his efforts to sell his book and create a "name" for himself on any speaking tour.

That said, Tiversa filed a complaint in federal court today citing a number of counts including but not limited to Defamation, Slander, Libel, and others against Mr. Daugherty and LabMD. Tiversa is not litigious and it was our hope that he would conduct himself appropriately after receiving the C&D in November of 2012. But again, he sees himself as Batman.

Here is the real series of events that occurred in this case:

Tiversa, as you know, downloads leaked information on behalf of clients, individual, corporate and/or federal. In the process of downloading information, we often get files that are not related to our clients but are nonetheless sensitive. We call this "dolphin in the tuna net"....for example, if we were looking for "Goldman Sachs" and our system finds a file with the term "Goldman" in it. The file may have the name "Henry Goldman" but our system just saw "Goldman" and downloaded it, in the event it related to Goldman Sachs. After the file would be downloaded, it would be reviewed by an Analyst which would determine that it was NOT related to Goldman Sachs, but it may or may not include SSNs or other sensitive information. This was the case with LabMD.

In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name "LabMD" in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable. We could have chosen to do nothing at all and pretend that we never saw the file. That approach would leave both LabMD and the 9000 victims at very high risk (and growing) of fraud and identity theft. Needless to say, we contacted the company to inform them of the file with their company name on it. After providing the file with all of the information that we had, the Mr. Daugherty asked us for additional information that we did not have. We told him that we could perform the services but it would take a few weeks and would cost about $15K. After hearing this, he asked us to send him the SOW for the services. 2-3 weeks after providing the SOW and not hearing anything in return, I reached out to Mr. Daugherty to see if he had any questions (re: SOW) and he told me never to contact him again with no further explanation. We didn't.

Tuck Business School at Dartmouth (and Professor Eric Johnson) used Tiversa in early 2006 for a research project to determine to what extent, if any, leaked financial documents were able to found on P2P networks. The research consisted of Dartmouth providing simple and straightforward search terms to Tiversa like "bank" and "account" to locate and download files using Tiversa's engine to a hard drive that Dartmouth owned and controlled. Tiversa only issued the searches but was not able to see the actual downloads. The downloads were stored on a hard drive that graduate students at Dartmouth were to later evaluate. Although Dartmouth was researching this using resources from a grant by DHS, Tiversa was not paid anything for our participation. The research was impactful and resulte in a number of articles being published. With the prior success of the financial research, Dartmouth wanted to followup with a second research project focused on medical information in 2008. Following the exact same procedure, the medical research was completed and widely published in early 2009. Again, Tiversa did not receive any compensation whatsoever for our part in the project. Upon reading the research paper, one of the many example files that were used to demonstrate the problem was the file in question with LabMD. Tiversa did not know that the file was included in the research as we did not see the downloads, only the search terms. Frankly, it was not surprising that the file was found because it was never addressed with LabMD therefore the file continued to spread across the P2P network.

I was called to testify before Congress twice in 2009, once in May and the second in July, as they were investigating breaches of security via P2P. At the directior Congress, Tiversa was asked to demonstrate the extent and severity of the problem. Tiversa then provided Congress with numerous, redacted, examples of file disclosure that affected government, private and public enterprises, and individuals. Shortly after the hearings, Tiversa was visited by the FTC. The senior representatives from the FTC wanted to see the non-redacted versions of the files discussed with Congress as one of their missions is to help consumers handle ID theft. When Tiversa asked what would happen if we refused to provide the information, the FTC stated that they would issue a Civil Investigative Demand (CID which acts as a federal subpoena to gain access to the information. We told them that they would need to do that and then we would provide the information in accordance with the subpoena. The FTC issued a subpoena that asked us to provide any file, regardless of source, that disclosed >100 SSNs. We provided over 100 files to the FTC in accordance with the federal subpoena and the LabMD file was still one of them as it remained on the P2P network. We had no insight/control as to what the FTC was going to do with the information once they received it. Tiversa was not compensated in any way for providing this information to the FTC.

Apparently, the FTC sent questionnaires to some, if not all, of the companies or organizations that breached the sensitive information. The FTC posted on its website a copy of a standard letter(s) that was sent, which is how we knew that they had sent a letter or letters. We had no further communication with the FT regarding the breaches or their investigations.

LabMD sued Tiversa/Dartmouth/Eric Johnson. Case was dismissed (all three times) for jurisdiction issues.

Mr. Daugherty starts writing his book about his problems and blames everyone but himself and his lax security measures at LabMD. He refuses to provide any information to the FTC questionnaire saying it's a "witch hunt."

To this date, I have not heard of Mr. Daugherty spending a single penny in notification or protection of ANY of the over 9000 cancer/medical patients in which he violated their privacy and well established HIPAA laws. He sees himself as the "victim" when he is actually the perpetrator. He intends to capitalize on his "victim" status by becoming "Batman" on a crusade for all Americans against government overreach.

The FTC sued Mr. Daugherty and LabMD last week for his non-compliance with a federal subpoena (CID). In the FTC complaint, it noted that over 500 people [of the 9000 in the LabMD file] have become victims of ID theft and fraud according to a Sacramento, CA Police Department investigation. I would suppose that multip states AG's offices could pursue litigation against LabMD and Mr. Daugherty as well for not notifying the individuals (that reside in the various states) that their information had been breached. It is a requirement in 47 of the 50 states. I also only suppose that it is matter of time before there will be a class action suit file against LabMD and Mr. Daugherty for the continued reckless breach of patient information.

Mr. Daugherty continues to hype his book, even going as far to have a cheesy trailer made about the book which is full of false statements regarding Tiversa and me. He continues to suggest that Tiversa is "government funded" which we are not, and never have been. Tiversa has only received one round of funding in 2006 by Adams Capital Management.

In my opinion, he needs to draw some connection between Tiversa, "hacking" and the government in an effort to sell his book and, more importantly, claim that he was not required to compensate the 9000 true victims of this story.

Tiversa filed a Defamation suit against LabMD and Mr. Daugherty in federal court on September 5, 2013.

Essentially, Tiversa was trying to help the 9000 people by informing LabMD that there was a problem. Unfortunately, LabMD took the "shoot/sue the messenger" approach.

TIVERSA

Forensic Investigation Report - LABMD0001

Prepared for LabMD

1.0 Introduction

Worldwide Peer-to-Peer ("P2P") file sharing networks are primarily used for sharing music, movies, and software. Unfortunately, they also commonly expose confidential and sensitive government, corporate and consumer documents. Employees, suppliers, contractors, agents, partners, and customers inadvertently disclose millions of confidential and sensitive documents on the P2P file sharing networks each year.

Once disclosed, these documents are publicly available to any individual using one of the 2,800+ different P2P file sharing programs and versions, most of which are free and publicly available. Disclosed files are routinely accessed by identity thieves, cyber criminals, terrorists, competitors, the media, shareholders, and others.

It must be emphasized that P2P file sharing networks are not part of the World Wide Web. P2P file sharing networks are entirely separate, internet-based networks with unique searches, files, and users. P2P networks are extremely large. In fact, more users search the P2P for information than the World Wide Web, with over 1.8 billion searches a day occurring on the P2P networks. It is also estimated that over 550 million users have file sharing applications, and internet service providers have stated that up to 70% of internet traffic is consumed solely by P2P networks.

The risks related to P2P compromises will only escalate as P2P use continues to grow – driven by increased broadband access, the explosion of digital content, and increasing numbers of tech-savvy individuals entering the workforce. From a data and information security standpoint, P2P compromises are among the most damaging since users unknowingly share hundreds of documents, sometimes every file resident on their machine, including Word, Excel, PowerPoint, PDF, e-mails, databases, and PST files. Once these documents are shared or exposed to the millions of P2P users, they tend to "virally spread" across the networks as users continuously download these files from each other and thereafter proceed to re-share these files themselves.

Tiversa's unique value is in its patented EagleVision X1™ technology which can view and access the P2P in real-time. Similar to how Google has indexed the World Wide Web, Tiversa has "centralized" the notoriously "decentralized" P2P file sharing networks. As such, Tiversa has the ability to detect and record user-issued P2P searches, access and download files available on the P2P networks, determine the actual disclosure source of documents, track the spread of files across the entire P2P networks, and remediate P2P file disclosures.

This Forensic Investigation Report summarizes the results and suggested actions of Tiversa's Forensic Investigation Services for Incident LABMD0001.

SECTION 1 - Customer Information	
Organization Name	N/A
Contact Name	N/A
Contact Phone	N/A
Contact Email	N/A
SECTION 2 - Incident Information	
Incident Number	LABMD0001
Related Incidents	N/A
Date of Report	6/4/2014
Severity	URGENT
SECTION 3 - Preliminary Disclosure Information	
IP Address	64.190.82.42
P2P Client	N/A
Disclosure Type	Internal
Disclosure Source	LabMD
Filename(s)	insuranceaging_6.05.071.pdf

SECTION 4 - Incident Summary

On 2/5/2008, Tiversa's systems detected 1 file being disclosed on P2P file sharing networks. The detected file appears to be a 1,718 page "*Insurance Aging*" Report relating to "*LABMD, INCORPORATED.*" The file contains patient information including Name, Social Security Number, DOB, Insurance Information, Billing Date Code/CPT, Billed Amount etc., relating to approximately 9,000 apparent patients.

The file appears to be emanating from the IP Address 64.190.82.42, which traces to Atlanta, Georgia, US.

Upon further analysis, 19 total files were detected being disclosed from this IP address on various dates between 3/7/2007 and 2/25/2008. The additional files include Insurance Benefits labels, LabMD login credentials (username and passwords) relating to web access for insurance companies, LabMD Insurance Verification Specialist Duties, blank forms relating to daily credit card transactions, LabMD Medical Records Request letters, LabMD Patient Appeal Authorization letters, LabMD Payment Posting Specialist Duties, a LabMD Employee Handbook, LabMD Employee Time Off Request forms, documents containing meeting notes and other related letters.

Upon reviewing the metadata and files emanating from this source, Tiversa believes the disclosure source may be an individual employed with LabMD.

2.0 Investigation Findings

2.1 Source Identification

The disclosure source appears to have emanated from IP address 64.190.82.42. As of 6/3/2014 this IP address is registered to CYPRESSCOM.NET (CYPRESS COMMUNICATIONS LLC), and appears to be located in Atlanta, Georgia, US. For details related to this IP address see Figure 2-1-1 below.

Figure 2-1-1:
Disclosure Source IP Address/ Geolocation

IP Address	64.190.82.42
Location	UNITED STATES, GEORGIA, ATLANTA
Latitude & Longitude	33.831847, -84.386614 (33°49'55"N 84°23'12"W)
Connection	CYPRESS COMMUNICATIONS LLC
Local Time	03 Jun, 2014 05:41 PM (UTC -04:00)
Domain	CYPRESSCOM.NET

Based on an initial investigation by Tiversa, the information found within the content and metadata of the files disclosed by this source indicate that the disclosure source may be an individual employed with LabMD.

There were 19 total files disclosed by this source. The file metadata (properties) of several of the documents list authoring ***Company*** as "*lab md*," and contain the following common identifiers within the file ***Author*** and ***Last Saved by*** fields:

rwoodson
sbrown
Administrator
Dan Carmichael
LabMD
Liz Fair

It is possible that these are user identifiers, providing additional evidence in that these users may have created or edited the disclosed documents, and that the documents may have been created or edited on a LabMD machine. See Figure 2-1-2 below for all file information.

Figure 2-1-2:
Disclosure Source IP Address - 64.190.82.42

File Title	Disclosure Date	Company	Author	Last Saved by
INSURANCE BENEFITS LABELS.doc	3/7/2007		Liz Fair	sbrown
WEB ACCESS FOR INSURANCE COMPANIES.doc	3/7/2007	LabMD		sbrown
LabMD Insurance Verification Specialist Duties.doc	3/7/2007		sbrown	sbrown
HELPFUL TIPS FOR BETTER AUDIT RESULTS.doc	3/15/2007		sbrown	sbrown
DAILY CREDIT CARD TRANSACTIONS.doc	10/11/2007		sbrown	sbrown
MEDICAL RECORDS FEE LTR.doc	11/10/2007	labmd	Administrator	sbrown
MEDICAL RECORDS RELEASE.doc	11/10/2007	labmd	Administrator	sbrown
MEDICAL RECORDS REQ LTR.doc	11/10/2007	labmd	Administrator	rwoodson
PATIENT APPEAL AUTHORIZATION LTR.doc	11/10/2007	labmd	Administrator	rwoodson
LabMD Payment Posting Specialist Duties.doc	11/10/2007		sbrown	rwoodson
Patient Locator Project.doc	11/13/2007		rwoodson	rwoodson
Humana patient Doc.doc	11/13/2007	labmd	rwoodson	rwoodson
Employee Handbbook.doc	11/15/2007		Dan Carmichael	
Employee Application Benefits.pdf	11/15/2007		a498584	
Employee Time Off Requests2007.doc	11/29/2007		rwoodson	rwoodson
insuranceaging_6.05.071.pdf	2/5/2008			
BCBS HMO & POS APPEAL LTR.doc	2/25/2008	labmd	Administrator	rwoodson
BCBS PAID PT LTR.doc	2/25/2008	labmd	Administrator	rwoodson
Roz's Coverage.doc	2/25/2008		rwoodson	rwoodson

One file emanating from this source appears to be a letter from the following individual:

Rosalind Woodson
Billing Manager/LabMD
rwoodson@labmd.org

This individual appears to be employed with LabMD and may have utilized the "*rwoodson*" user identifier as referenced within the metadata of the disclosed documents.

One of the additional files emanating from this source appears to be a Medical Records Request letter from the following individual:

Sandra Brown
Billing Manager/LabMD
*(678) 443-2338 *Direct**
sbrown@labmd.org

This individual appears to be employed with LabMD and may have utilized the "*sbrown*" user identifier as referenced within the metadata of the disclosed documents.

Given these findings, it is possible that Rosalind Woodson or Sandra Brown may have disclosed the documents utilizing a P2P file sharing application from a work or home computer. It should be noted that the 1,718 page "*Insurance Aging*" Report (*insuranceaging_6.05.071.pdf*) was detected being disclosed on P2P file sharing networks on 2/5/2008. A total of 19 files were detected being disclosed on P2P file sharing networks between 3/7/2007 - 2/25/2008 from the IP Address 64.190.82.42.

See Figure 2-1-3 below for a sample of redacted screenshots of the documents emanating from this source.

Figure 2-1-3:

Insurance Aging

LABMD, INCORPORATED

LABMD

Report Options
6/5/2007 12:07:11PM

Option	Value
Age From	06/05/2007
Show Billing History	All dates Billed
Sort Insurance By	Insurance Code
Show Summary Only	No
Show Billing Detail	Yes
Subtotal by Billing	No
Subtotal by Provider	Yes

Insurance Aging

LABMD, INCORPORATED

LABMD

HUMANA P O BOX 14601, LEXINGTON, KY 40233 (502) 580-5050

JOSEF Date of Birth: Insured: Self
Insurance: Primary ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total

Patient Total:

CLAUDETTE Date of Birth: Insured: Self
Insurance: Primary Group Number: ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total

Patient Total:

Insurance Total:

TRICARE PO BOX 7890, MADISON, WI 53707 (800) 403-3950

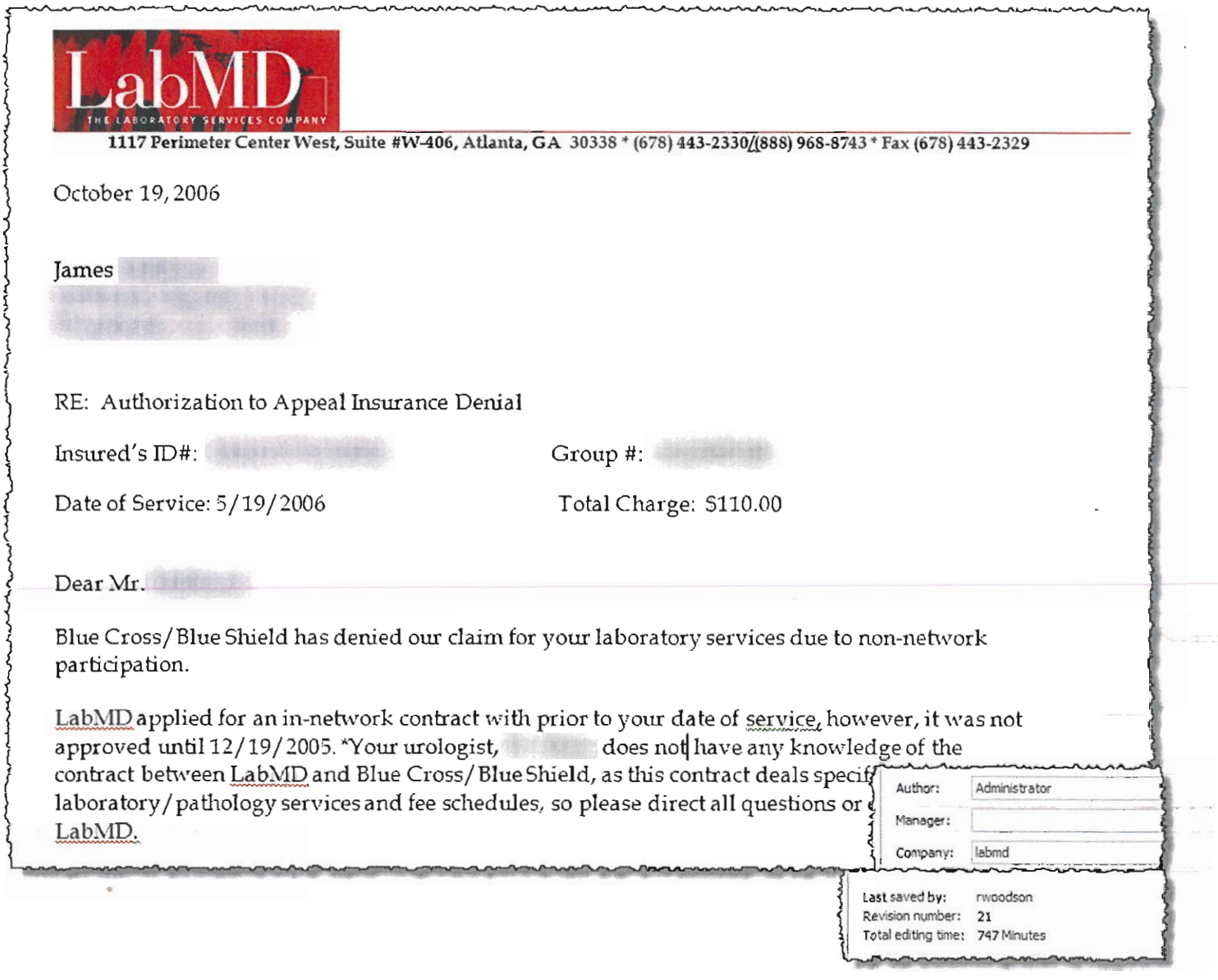
TOMMY Date of Birth: Insured: Self
Insurance: Secondary ID:

Billing	Date	Code/CPT	Billed	Amount	Current	31-60	61-90	91-120	> 120	Total

Patient Total:

Printed 6/5/2007 12:07:11PM Page 1718 of 1718

Figure 2-1-4:



LabMD
THE LABORATORY SERVICES COMPANY

1117 Perimeter Center West, Suite #W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 968-8743 * Fax (678) 443-2329

October 19, 2006

James

RE: Authorization to Appeal Insurance Denial

Insured's ID#: Group #:

Date of Service: 5/19/2006 Total Charge: $110.00

Dear Mr.

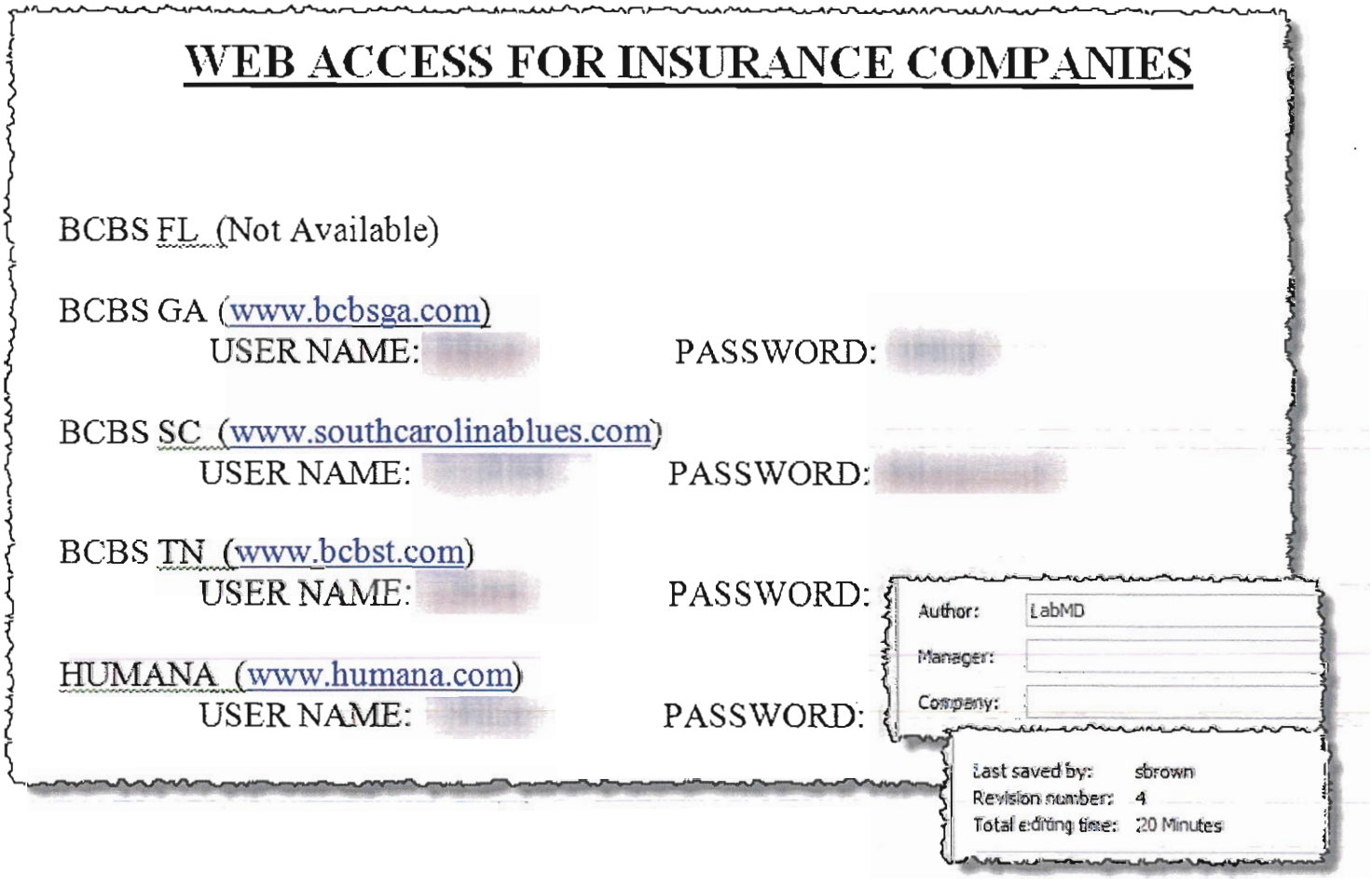
Blue Cross/Blue Shield has denied our claim for your laboratory services due to non-network participation.

LabMD applied for an in-network contract with prior to your date of service, however, it was not approved until 12/19/2005. *Your urologist, does not have any knowledge of the contract between LabMD and Blue Cross/Blue Shield, as this contract deals specif laboratory/pathology services and fee schedules, so please direct all questions or LabMD.

Author: Administrator
Manager:
Company: labmd

Last saved by: rwoodson
Revision number: 21
Total editing time: 747 Minutes

Figure 2-1-5:



WEB ACCESS FOR INSURANCE COMPANIES

BCBS FL (Not Available)

BCBS GA (www.bcbsga.com)
USER NAME: PASSWORD:

BCBS SC (www.southcarolinablues.com)
USER NAME: PASSWORD:

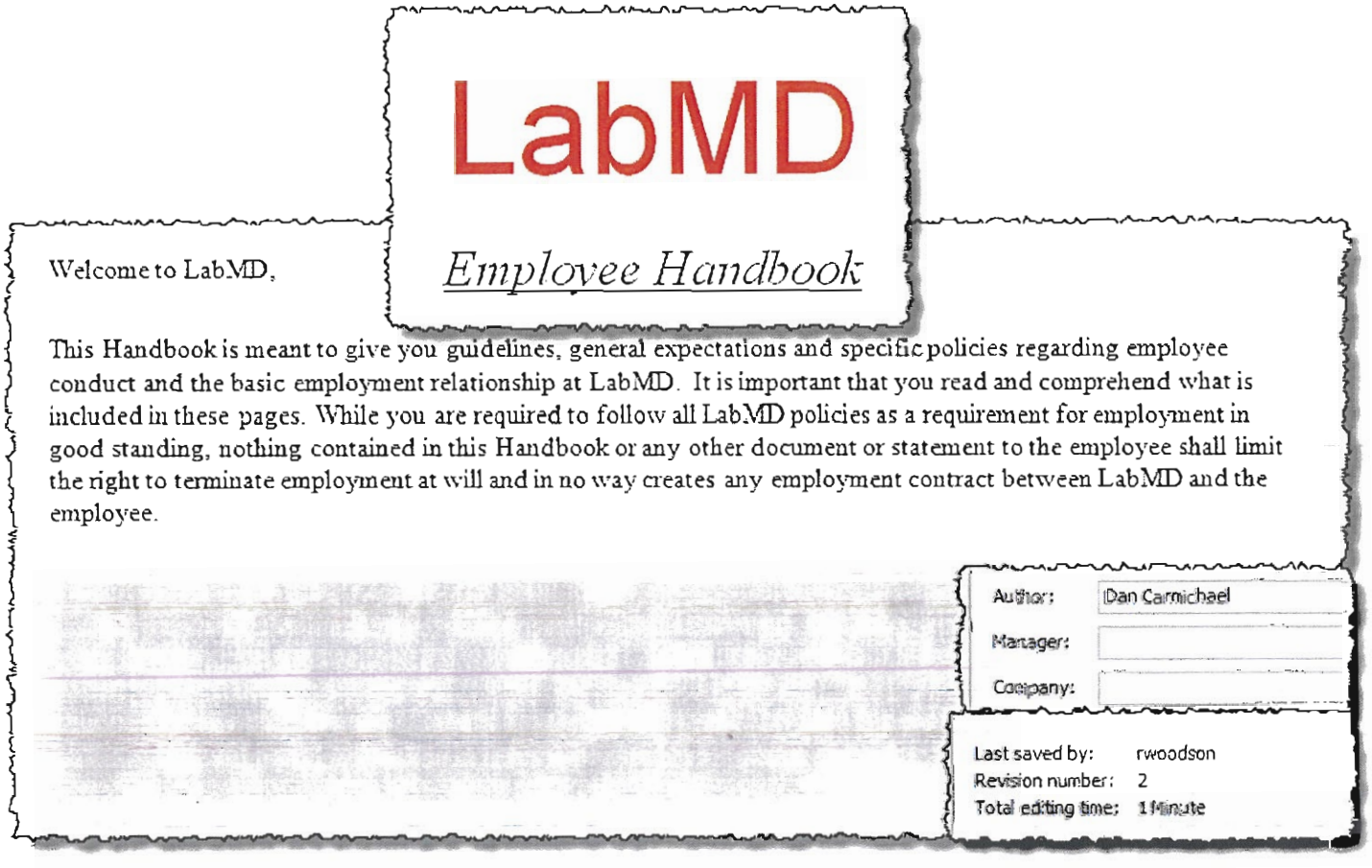
BCBS TN (www.bcbst.com)
USER NAME: PASSWORD:

HUMANA (www.humana.com)
USER NAME: PASSWORD:

Author: LabMD
Manager:
Company:

Last saved by: sbrown
Revision number: 4
Total editing time: 20 Minutes

Figure 2-1-6:



LabMD

Employee Handbook

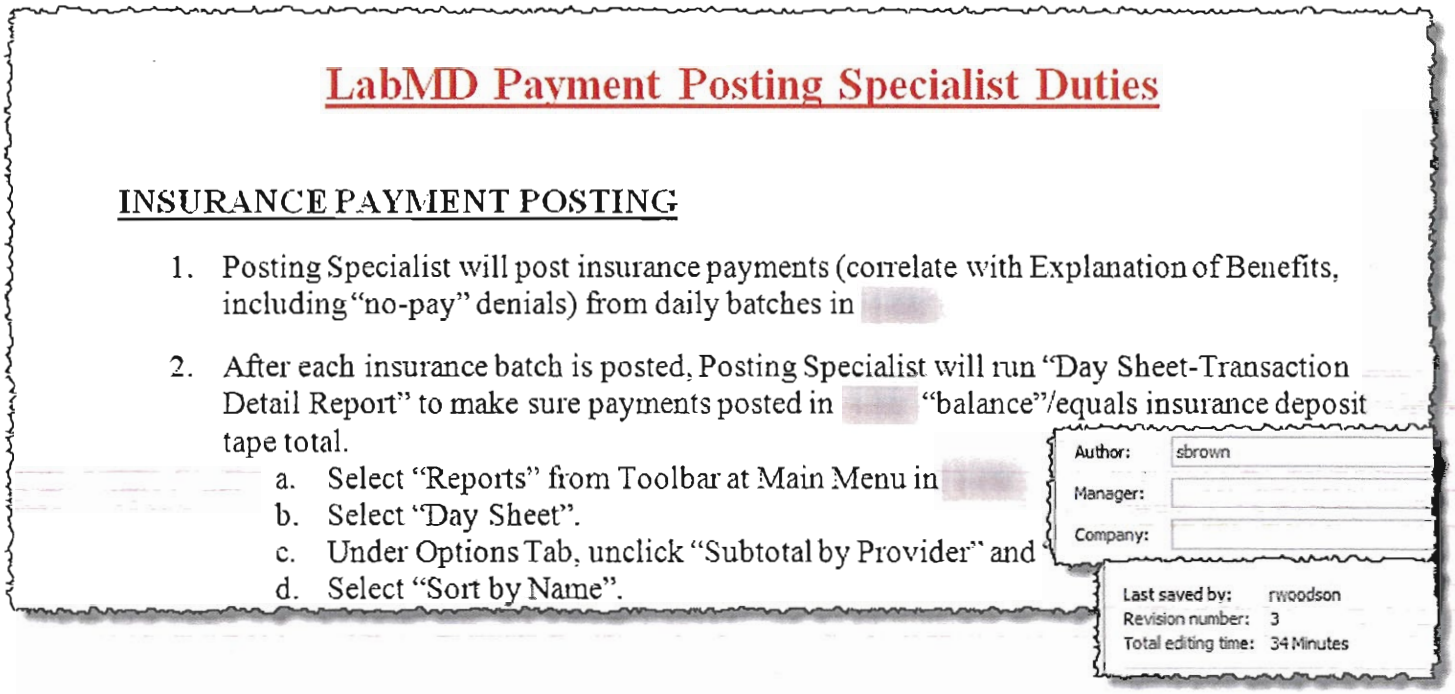
Welcome to LabMD,

This Handbook is meant to give you guidelines, general expectations and specific policies regarding employee conduct and the basic employment relationship at LabMD. It is important that you read and comprehend what is included in these pages. While you are required to follow all LabMD policies as a requirement for employment in good standing, nothing contained in this Handbook or any other document or statement to the employee shall limit the right to terminate employment at will and in no way creates any employment contract between LabMD and the employee.

Author: Dan Carmichael
Manager:
Company:

Last saved by: rwoodson
Revision number: 2
Total editing time: 1 Minute

Figure 2-1-7:



LabMD Payment Posting Specialist Duties

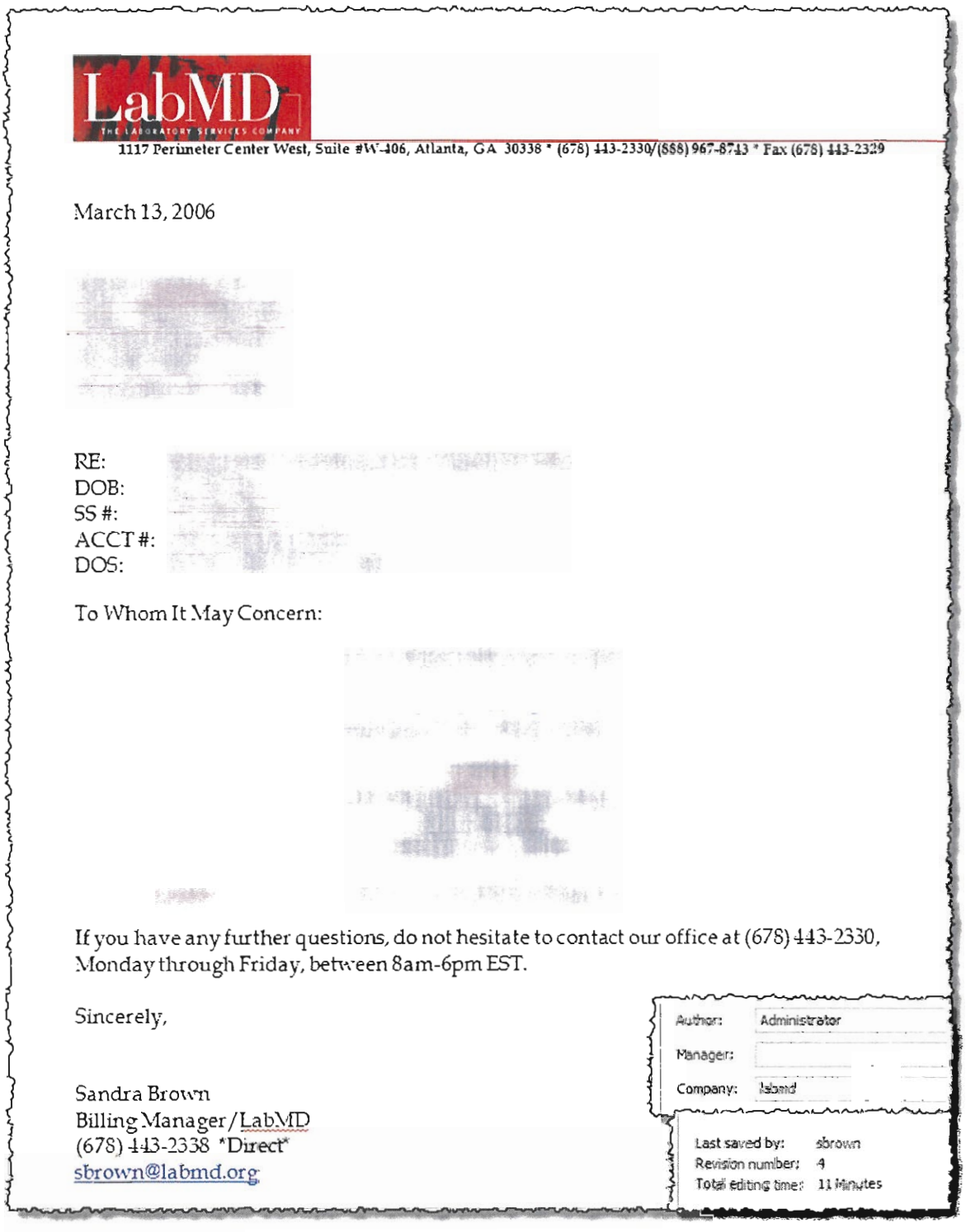
INSURANCE PAYMENT POSTING

1. Posting Specialist will post insurance payments (correlate with Explanation of Benefits, including "no-pay" denials) from daily batches in
2. After each insurance batch is posted, Posting Specialist will run "Day Sheet-Transaction Detail Report" to make sure payments posted in "balance"/equals insurance deposit tape total.
   a. Select "Reports" from Toolbar at Main Menu in
   b. Select "Day Sheet".
   c. Under Options Tab, unclick "Subtotal by Provider" and
   d. Select "Sort by Name".

Author: sbrown
Manager:
Company:

Last saved by: rwoodson
Revision number: 3
Total editing time: 34 Minutes

Figure 2-1-8:



LabMD
THE LABORATORY SERVICES COMPANY

1117 Perimeter Center West, Suite #W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 967-8743 * Fax (678) 443-2329

March 13, 2006

[redacted]

RE: [redacted]
DOB:
SS #:
ACCT #:
DOS:

To Whom It May Concern:

[redacted]

If you have any further questions, do not hesitate to contact our office at (678) 443-2330, Monday through Friday, between 8am-6pm EST.

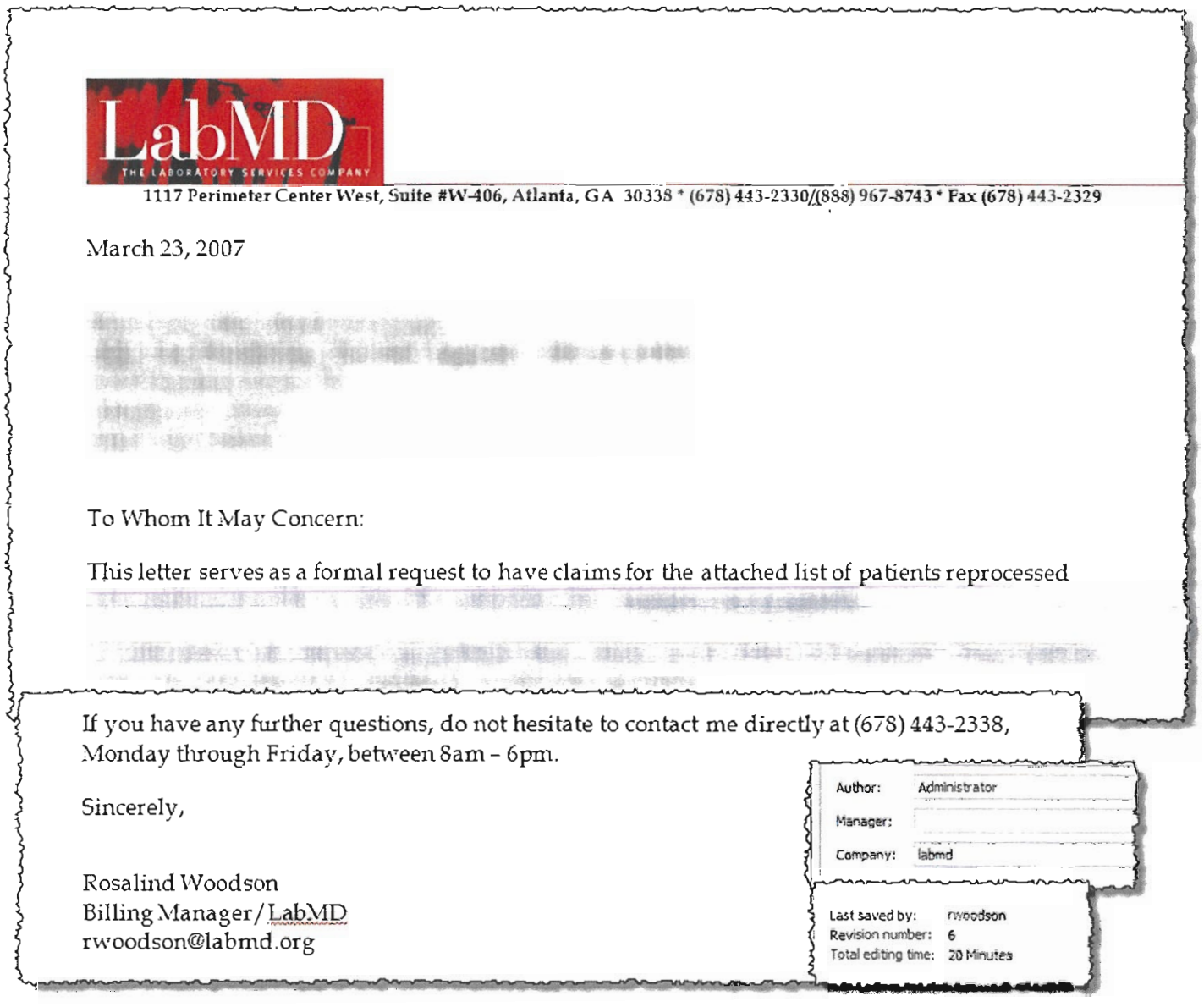
Sincerely,

Sandra Brown
Billing Manager/LabMD
(678) 443-2338 *Direct*
sbrown@labmd.org

Author: Administrator
Manager:
Company: labmd

Last saved by: sbrown
Revision number: 4
Total editing time: 11 Minutes

Figure 2-1-9:



LabMD
THE LABORATORY SERVICES COMPANY

1117 Perimeter Center West, Suite #W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 967-8743 * Fax (678) 443-2329

March 23, 2007

[redacted]

To Whom It May Concern:

This letter serves as a formal request to have claims for the attached list of patients reprocessed

[redacted]

If you have any further questions, do not hesitate to contact me directly at (678) 443-2338, Monday through Friday, between 8am - 6pm.

Sincerely,

Rosalind Woodson
Billing Manager/ LabMD
rwoodson@labmd.org

Author: Administrator
Manager:
Company: labmd

Last saved by: rwoodson
Revision number: 6
Total editing time: 20 Minutes

2.2 File Spread Analysis

In addition to the above disclosure source identification and geolocation analysis, Tiversa also performed a file spread analysis to determine if any of the LabMD-related files have spread, and were acquired by any other users of P2P networks. Based on this analysis, Tiversa detected (6) additional IP addresses disclosing one or more of the files originally detected emanating from 64.190.82.42.

See Figure 2-2-1 below for a summary table of all IP addresses detected.

Figure 2-2-1:
File Spread Analysis – IP Summary Table

Source#	IP Address	Disclosure Date(s)	ISP	Geolocation**	Total Files
Source 1	64.190.82.42*	3/7/2007 - 2/25/2008	CYPRESS COMMUNICATIONS LLC	ATLANTA, GEORGIA, US	19
Source 2	68.107.85.250	2/5/2008 - 9/20/2011	COX COMMUNICATIONS INC.	SAN DIEGO, CALIFORNIA, US	3,302
Source 3	173.16.83.112	11/5/2008 - 2/14/2009	MEDIACOM COMMUNICATIONS CORP	CHICAGO, ILLINOIS, US	1,832
Source 4	201.194.118.82	4/7/2011	SAN JOSE (SANJOSECA.GOV)	SAN JOSE, SAN JOSE, CR	33
Source 5	90.215.200.56	6/9/2011	EASYNET LTD	LONDON, ENGLAND, UK	47
Source 6	71.59.18.187	5/5/2010 - 11/7/2012	COMCAST CABLE COMMUNICATIONS HOLDINGS INC	ALPHARETTA, GEORGIA, US	254
Source 7	173.16.148.85	2/23/2009 - 11/7/2012	MEDIACOM COMMUNICATIONS CORP	NASHVILLE, TENNESSEE, US	520

**Indicates original disclosure source IP reported in Incident LABMD0001*
***All IP Geolocation information associated with these IP addresses was discovered as of 6/3/2014.*

The 6 additional IP addresses were detected in possession of the 1,718 page "Insurance Aging" Report (*insuranceaging_6.05.071.pdf*) on various dates within the disclosure date ranges referenced above.

These 6 IP addresses possess additional files including federal tax returns relating to numerous individuals, credit reports, credit card and bank account statements, passports, usernames and passwords to online accounts, medical payment data, lists of credit card numbers, social security numbers, instructions on how to hack and steal passwords etc. Tiversa classifies these 6 additional IP addresses as Information Concentrators.

Throughout our extensive P2P research, Tiversa continues to see individuals harvesting a large number of files containing confidential and sensitive data. Tiversa calls these individuals "Information Concentrators" and in most cases, they are suspicious in nature. These individuals utilize P2P file sharing networks to search for sensitive and confidential data (i.e. Credit Card #'s, Passwords, Account #'s, SSN, PII, Payroll Information, HR, Medical, Financial, IT Information etc). Information Concentrators gather this information and could potentially use it for malicious purposes.

For a complete list of file titles detected in possession of these additional IP addresses, see the excel file titled "LABMD0001_Forensic_Investigation_Report_File_Spread_Analysis.xls", which is provided along with this report.

3. Conclusions/Suggested Actions

In order to contain any further proliferation of these LabMD-related files across the P2P networks, any computers responsible for their disclosure must be identified and then removed from the P2P networks – or at a minimum, the LabMD related files must be removed from the suspect's machine.

Based on the information reviewed by Tiversa, a suggested course of action is to contact the apparent LabMD employees listed within the Investigation findings above (Rosalind Woodson and Sandra Brown) reference the disclosed document titles, document content, and the supporting evidence listed above. It is possible that an investigation into these disclosed files and possible sources will allow LabMD to determine the disclosure source. If the disclosure source machine is found, the machine should be reviewed for the presence of file sharing software. An investigation of this machine should indicate that the files found on that machine match the file listing noted in Figure 2-1-2 above. It should be noted that the disclosure source machine may be a home computer, work computer or possibly a laptop.

Additional remediation activities can be discussed with Tiversa once additional investigation steps by LabMD have been completed.

[redacted]

Tiversa
606 Liberty Avenue
Pittsburgh, PA 15222

(724) 940-9030 *office*
(724) 940-9033 *fax*

www.tiversa.com