

professional audits every two years for the next 20 years. The proposed order also would require LabMD to notify consumers whose information was compromised.

LabMD founder Michael Daugherty has objected to these terms and has been fighting the FTC investigation for several years. He claims on his personal website that LabMD is a victim of theft by a cybersecurity firm that he says was trying to sell his company services. Daugherty says that when he refused, the stolen data was supplied to government regulators, who are using the leak to punish him as a small business owner and justify additional government regulation. Daugherty has written a book on the subject that he says will be published in September.

The trade commission's "enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority to engage in an ongoing witch hunt against private businesses," LabMD said in its statement.

According to the FTC complaint, a LabMD spreadsheet with insurance billing data on more than 9,000 consumers was discovered on a public file-sharing network. The spreadsheet contained Social Security numbers, birth dates, insurance information and medical treatment codes. The FTC says California police later discovered that identity thieves had acquired personal data from at least 500 LabMD consumers.

In its complaint, the FTC said lax security controls at LabMD resulted in the leak of the spreadsheet. Regulators say the company did not maintain a "comprehensive data security program" or use "readily available measures" to identify common vulnerabilities. The company also did not adequately train employees or prevent unauthorized access, according to the FTC.

RELATED

Judge: No estate rights for NY mom who killed kids

Electrical issues stall NSA data warehouse opening

Zimbabwe's top rights lawyer acquitted

Gov't delays US home construction data again

Top 7 Credit Cards For Those With Excellent Credit

Ad

15 NFL Cheerleaders Who Should Put on More Clothes

Ad

Zemanta

Tags

Government and politics, Business, United States government, General news, Crime, Social affairs, Social issues, Identity theft, Human rights and civil liberties, Computing and information technology, Technology, Technology issues, Health, Data privacy, Health issues, Computer and data security, Federal Trade Commission, Medical technology, Patient privacy, Patient rights, Medical informatics

Comments

[eSecurityPlanet](#) > [Network Security](#) > [FTC Claims LabMD Failed to Protect Consumers' Personal Data](#)

FTC Claims LabMD Failed to Protect Consumers' Personal Data

More than 9,500 customers' names and Social Security numbers were found on a P2P network and in the hands of identity thieves.

By **Jeff Goldman** | August 30, 2013

Share      



The Federal Trade Commission recently [filed a complaint](#) against the Atlanta-based medical testing laboratory LabMD, claiming that the company failed to protect consumers' personal data, including their medical information.

According to the complaint, a LabMD spreadsheet containing 9,000 consumers' names, Social Security numbers, birthdates, health insurance information and medica treatment codes was found on a P2P file-sharing network.

In a separate incident, California's Sacramento Police Department found LabMD documents containing at least 500 consumers' names, Social Security numbers, and in some instances, bank account information, were found in the possession of identity thieves.

Among other things, the complaint alleges that LabMD "did not implement or maintain a comprehensive data security program to protect this information; did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information; did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs; did not adequately train employees on basic security practices; and did not use readily available measures to prevent and detect unauthorized access to personal information."

The complaint proposes that LabMD be required to implement a comprehensive information security program, and have that program evaluated every two years by an independent, certified security professional for the next 20 years.

"The unauthorized exposure of consumers' personal data puts them at risk," Jessica Rich, Director of the FTC's Bureau of Consumer Protection, said in a [statement](#). "The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users."

  Loading Comments...

Comment and Contribute

Name

Displayed next to your comment

White Papers

eBooks

Endpoint Buyers Guide



It takes more than antivirus to s... important part of your IT securit

The Convergence of Reputational Risk and IT Out



Today, your company's digital p... assets are vulnerable to securi

Understanding Data Security & Trends and



Live Event Date: January 09, 20... business imperative. As we se

Most Recent Network Security Articles

- » [Akamai Beefs up DDoS Security with Prolexic Buy](#)
December 02, 2013
- » [Data Breach at UW Medicine Exposes 90,000 Patients' Information](#)
November 29, 2013
- » [University of Pittsburgh Medical Center Acknowledges Privacy Breach](#)
November 29, 2013
- » [Data Breach at Florida Medical Group Exposes 4.400 Patients' Personal Data](#)



Response Breaches Forensics Governance ID Theft Preparedness Litigation Technology

News Blogs Interviews Webinars White Papers Memberships Resources Events Jobs

Home > Articles

FTC Complaint Leads Breach Roundup

Lab Accused of Failing to Protect Patient Information

By Jeffrey Roman, September 5, 2013. Follow Jeffrey @ISMG_News

★ Credit Eligible Email Tweet Like Share



In this week's breach roundup, the Federal Trade Commission has filed a complaint against LabMD Inc., alleging that the Atlanta-based medical testing laboratory failed to protect personal information for about 10,000 consumers. Also, the number of individuals affected by a Department of Energy breach first reported in late August is larger than originally suspected.

Lab Cited in FTC Complaint

The **Federal Trade Commission** has filed a complaint against LabMD Inc., alleging that the Atlanta-based medical testing laboratory failed to protect personal information for about 10,000 consumers.

The FTC alleges that LabMD billing information for more than 9,000 consumers contained in a spreadsheet was found on a peer-to-peer file-sharing network. That incident occurred in 2008, before the HIPAA breach notification rule went into effect, according to an FTC spokesperson. Compromised information includes names, Social Security numbers, dates of birth, health insurance information and medical treatment codes.

The complaint also alleges that in 2012, LabMD documents containing sensitive information about at least 500 consumers was found in the hands of identity thieves. That information included names, Social Security numbers, and, in some cases, bank account information.

The FTC describes a proposed order that would require LabMD to implement a comprehensive information security program and have it evaluated every two years by an independent security professional over a period of 20 years.

The allegations established in the complaint will be tried during a formal hearing before an administrative law judge.

The FTC and the Department of Health and Human Services can both get involved with investigations of health data breaches, an FTC spokesperson explained. In general, FTC

RELATED CONTENT

- [NSA Outlines Steps to Reduce Leaks](#)
- [9/11 DDoS Alert for Banks, Agencies](#)
- [Regulations' Impact on Data Breach Costs](#)
- [An Adversarial View of Security](#)
- [Collaboration Enhances Fraud Detection](#)

RELATED WHITEPAPERS

- [Implementing DSD'S Top 35 Mitigation Strategies](#)
- [25 Years of Vulnerabilities: 1988-2012](#)
- [Real-Time Malware Protection for Financial Institutions](#)
- [Rethinking your Enterprise Security](#)
- [The Bot Threat](#)

Get Daily Email Updates

Report a Breach

Are you aware of a data breach that has not yet been reported? Alert our news team.

Solutions

INTERVIEW

[DDoS: What to Expect Next](#)

WEBINAR

[The Analyst's Eye: Top Fraud Threats to Watch in 2014](#)

WHITEPAPER

[Buyer's Criteria for Advanced Malware Protection](#)

[More solutions...](#)

Recent Content

Most Popular

1. [Questioning the Culture of Surveillance](#)
2. [Improving Cyberthreat Info Sharing](#)
3. [Cloud Security: Top 10 Tips](#)
4. [Evolution of Attackers-for-Hire](#)
5. [Using Big Data to Prevent Fraud](#)
6. [Twitter Adds Enhanced Encryption](#)
7. [Dating Site Breach Leads Roundup](#)
8. [How to Fight Cross-Border ATM Fraud](#)
9. [Breach Trend: Fewer Business Associates](#)
10. [Shaming China to Stop Hacks Doesn't](#)

[View more...](#)

Featured Jobs

"has broad authority related to remediation" in data security, the spokesperson said.

Dept. of Energy Breach Affects 53,000

The number of individuals affected by a [Department of Energy](#) breach first reported in late August is larger than originally suspected.

The department now confirms that the breach, first reported to have impacted 14,000 current and former agency employees, actually affected 53,000 [see: [Dept. of Energy Hit by Hackers](#)].

Names, Social Security numbers and dates of birth for current and past federal employees, including dependents and contractors, were compromised in the incident, the department said.

"Based on the findings of the department's ongoing investigation into this incident, we do believe PII theft may have been the primary purpose of the attack," the statement said.

Affected individuals are being offered assistance on steps to take to protect themselves against potential fraud or [identity theft](#).

DoE says it's cybersecurity office, the Office of Health, Safety and Security and the inspector general's office are working with federal law enforcement to investigate the breach. "Once the full nature and extent of this incident is known, the department will implement a full remediation plan," the DoE statement says.

UK Breach Leads to Fine

The UK Information Commissioner's Office has fined the [Aberdeen City Council](#), located in Northeast Scotland, £100,000 as a result of sensitive personal information relating to social services being published online.

A council employee accessed documents from a home computer, and a file transfer program installed on the machine automatically uploaded the documents to a website, posting sensitive information about several vulnerable children and their families, including details of alleged criminal offenses, the ICO reports.

The files were uploaded in November 2011 and remained online until February 2012, the ICO said.

In its investigation, the ICO found that the council had no policy for employees working from home, and didn't have sufficient measures in place to restrict downloading sensitive information from the council's network.

View the [monetary penalty notice](#).

Missing Laptop Contained Patient Info

| 1 | 2

Next »

View on 1 page »

Follow Jeffrey Roman on Twitter: [@ISMG_News](#)



Email



Tweet



Like



Share



Get Permission

Please enable JavaScript to view the [comments powered by Disqus](#).

ARTICLE

Battling Cybercrime Globally

The State Department's top cyberdiplomat, Chris Painter, explains how the United States is helping...

Oversight & Control - Information Risk Manager Lead - Technology Risk Practitioner, Executive Direct

JPMorgan Chase - New York, NY

Manager, Information Risk & Security Officer (IRSO)

KPMG - Toronto, Ontario

Senior Healthcare Information Privacy Specialist

FairWarning, Inc - Clearwater, FL

Information Risk Management Specialist

University of Colorado - Boulder, CO

CIB - Information Risk Manager - VP

JP Morgan Chase - Chicago, IL

[View our Job Board for more...](#)

From Our Sponsors

Why You Need a Next-Generation Firewall



Mapping Security for your Virtual Environment

Key Benefits of Application White-Listing and How to Achieve Them

Upcoming Webinars

Continuous Monitoring: How to Get Past the Complexity

DECEMBER 4, 2013 @ 10:00 AM EASTERN

Fraud Prevention: Utilizing Mobile Technology for Authentication & Transaction Verification

DECEMBER 9, 2013 @ 1:30 PM EASTERN

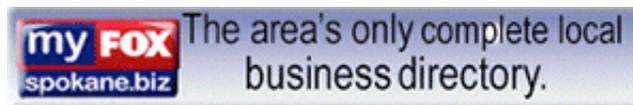
[More webinars...](#)



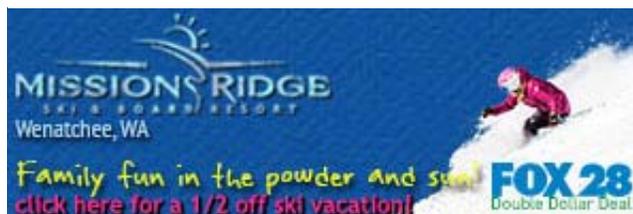
- ▼ My FOX ▼
- News ▼
- Weather ▼
- Sports ▶
- Contests ▼
- Events ◦
- Syncbak

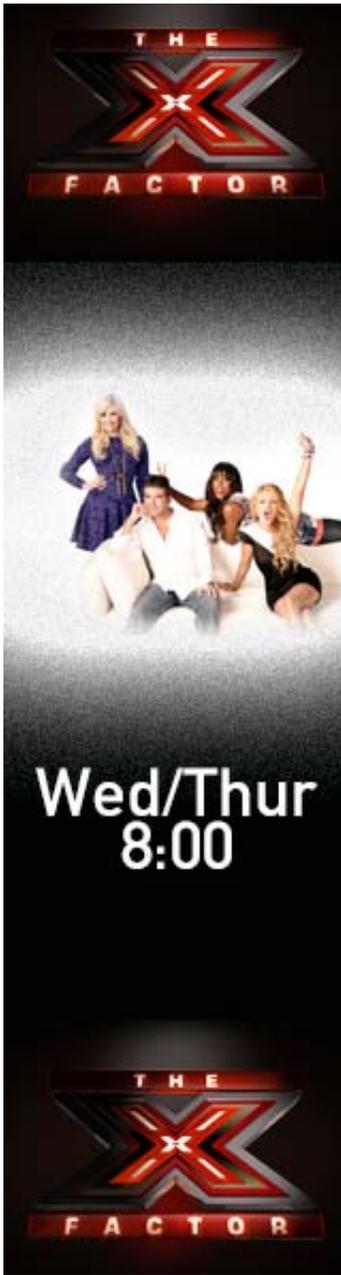
[Home](#) / [FTC: Medical lab's lax security led to data leak](#)

FTC: Medical lab's lax security led to data leak



 <p>Healing Art Therapeutic Massage Clinic LLC</p>	<p>Healing Art Therapeutic Massage Clinic - 1 hour massage \$35</p>
---	--





Tweet 38
Like 296
g+1 12
Share 6

Submitted by [Fox First at Ten](#) on August 29th
 By ANNE FLAHERTY Associated Press

WASHINGTON (AP) - The Federal Trade Commission on Thursday accused a small Atlanta-based medical lab that specializes in cancer detection of not doing enough to protect its patients' online records, resulting in the leak of Social Security numbers and birth dates of more than 9,000 consumers.

The complaint against LabMD describes what many consumers fear: being forced to hand over personal information to a doctor's office or hospital, not knowing how that data is handled or who has access to it, only to become vulnerable to identity theft. The allegations also raise questions about the federal government's push for the health care industry to swap paper for electronic records to save money when doing so relies on cybersecurity investments by private companies.

In a statement, LabMD said the company "looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes."

Bloomberg Businessweek**News**

<http://www.businessweek.com/ap/2013-08-29/ftc-medical-labs-lax-security-led-to-data-breach>

FTC: Medical lab's lax security led to data leak

By Anne Flaherty August 29, 2013

WASHINGTON (AP) — The Federal Trade Commission on Thursday accused a small Atlanta-based medical lab that specializes in cancer detection of not doing enough to protect its patients' online records, resulting in the leak of Social Security numbers and birth dates of more than 9,000 consumers.

The complaint against LabMD describes what many consumers fear: being forced to hand over personal information to a doctor's office or hospital, not knowing how that data is handled or who has access to it, only to become vulnerable to identity theft. The allegations also raise questions about the federal government's push for the health care industry to swap paper for electronic records to save money when doing so relies on cybersecurity investments by private companies.

In a statement, LabMD said the company "looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes."

Jessica Rich, director of the FTC's bureau of consumer protection, said LabMD's practices put consumers at serious risk of identity theft.

"The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users," she said in a statement.

More than half of doctors' offices and 4 out of 5 hospitals have transitioned from paper to electronic medical records, according to the government. Moving to computerized records is the rare consensus issue in health care, enjoying support from across the political spectrum. Taxpayers have already contributed more than \$14 billion to help speed the move through an incentive program that was part of the Obama administration's economic stimulus package.

The hope was that going digital would make caring for patients safer and less costly by helping avoid medical mistakes and cutting down on duplicative tests. But concerns have also surfaced about patient privacy and vulnerability to fraud. And progress has been mixed in getting medical computers from different offices to talk to each other, the key to a seamlessly efficient system.

A pair of reports in 2011 by the Health and Human Services inspector general warned that the drive to connect hospitals and doctors electronically was being layered on top of a system that already has privacy problems. The administration said in response it would pursue stronger safeguards.

The complaint filed Thursday means that the allegations will be tried in a formal hearing before an administrative law judge. The FTC wants the judge to order LabMD to institute a comprehensive information security program with professional audits every two years for the next 20 years. The proposed order also would require LabMD to notify consumers whose information was compromised.

LabMD founder Michael Daugherty has objected to these terms and has been fighting the FTC investigation for several years. He claims on his personal website that LabMD is a victim of theft by a cybersecurity firm that he says was trying to sell his company services. Daugherty says that when he refused, the stolen data was supplied to government regulators, who are using the leak to punish him as a small business owner and justify additional government regulation. Daugherty has written a book on the subject that he says will be published in September.

The trade commission's "enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority to engage in an ongoing witch hunt against private businesses," LabMD said in its statement.

According to the FTC complaint, a LabMD spreadsheet with insurance billing data on more than 9,000 consumers was discovered on a public file-sharing network. The spreadsheet contained Social Security numbers, birth dates, insurance information and medical treatment codes. The FTC says California police later discovered that identity thieves had acquired personal data from at least 500 LabMD consumers.

In its complaint, the FTC said lax security controls at LabMD resulted in the leak of the spreadsheet. Regulators say the company did not maintain a "comprehensive data security program" or use "readily available measures" to identify common vulnerabilities. The company also did not adequately train employees or prevent unauthorized access, according to the FTC.

©2013 Bloomberg L.P. All Rights Reserved. Made in NYC

HealthITSecurity
News and Resources for HealthIT Security Pros

Download The Latest White Papers And Webcasts On:

- BYOD
- Single Sign On
- Data Security
- HIPAA Compliance
- And More

VISIT THE HEALTH IT SECURITY WHITE PAPER LIBRARY TODAY.

Home News Topics White Papers Health IT Terms Newsletter

HIPAA and Compliance EHR Security HIE Security Mobile Security Data Breaches Cloud Security Privacy

Home > Articles > FTC files LabMD patient privacy complaint; LabMD responds

FTC files LabMD patient privacy complaint; LabMD responds

Author Name **Patrick Ouellette** | Date **August 30, 2013** | Tagged **Administrative Safeguards**, **Data Breach Management**, **Health Data Breach**, **Health Data Encryption**, **Health Data Security**, **Technical Safeguards**

Like Tweet

5



SherWeb

Need help complying with the HIPAA regulations?

WE HAVE THE RIGHT SOLUTION FOR YOU!

Become HIPAA compliant NOW!

As a result of LabMD, Inc. allegedly failing to reasonably protect the security of consumers' personal data, including medical information, the **Federal Trade Commission (FTC)** filed a **complaint** this week. LabMD, a cancer detection **facility**, offers analysis and diagnosis of blood, urine, and tissue specimens for cancers, micro-organisms and tumor markers.

The FTC maintains that LabMD had exposed more than 9,000 patients' data over a peer-to-peer (P2P) file-sharing network and failed to accomplish these items:

- Implement or maintain a comprehensive data security program to protect this information
- Use readily-available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information
- Did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs
- Did not adequately train employees on basic security practices
- Did not use readily available measures to prevent and detect unauthorized access to personal information

"The unauthorized exposure of consumers' personal data puts them at risk," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate **security measures** to prevent it from falling into the hands of identity thieves and other unauthorized users."

LabMD responded to the FTC's complaint by describing it as a "witch hunt" and said that the FTC's action is a clear example of federal government overreach. LabMD made this statement, **according to PHIPrivacy.net**:

The Federal Trade Commission's enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority to engage in an ongoing witch hunt against private businesses. The allegations in the FTC's complaint are just that: allegations. LabMD looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes.

The FTC has repeatedly overstepped its statutory authority under Section 5 of the Federal Trade Commission Act and the FTC does not have the authority to bring this enforcement action.

HealthIT Security Watch

Stay informed with our industry-leading weekly email

Email

[sign up](#)



HealthITAnalytics

Get The Latest News And Real Word Advice On:

- Predictive Analytics
- Healthcare BI
- Patient Care
- Big Data
- Population Health

Visit [HealthITAnalytics.com](#) And Sign Up For Our **FREE** Newsletter To Hear From HIM Directors, CIO's And Informaticists On How They Are Using Analytics In Their Hospitals.

Most Popular Topics

- HIPAA
- Health Data Encryption
- Health Data Breach
- Health Data Security
- Technical Safeguards
- Administrative Safeguards
- PHI

Sep 12 2013

FTC reveals provisionally redacted complaint against LabMD

Article or Commentary, Breaches, U.S. breaches

The Federal Trade Commission has released a provisionally redacted public version of its [complaint against LabMD](#) (PHIprivacy.net's coverage of LabMD linked [here](#)).

Intriguingly, the complaint cites another situation that appears to be unrelated to the "1718 file" incident:

In October 2012, the Sacramento, California Police Department found more than 35 Day Sheets and a small number of copied checks in the possession of individuals who pleaded no contest to state charges of identity theft. These Day Sheets include personal information, such as names and SSNs, of several hundred consumers in different states. Many of these consumers were not included in the P2P insurance aging file, and some of the information post-dates the P2P insurance aging file. A number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves.

The inclusion of this information may be used to demonstrate that the Limewire incident was not an isolated security failure and that LabMD likely had at least one other security incident. Inspection of the Appendix to the complaint reveals that the day sheets were dated between 2007 and March, 2009 (well after the "1718 File" P2P incident). I contacted LabMD for additional details on what appears to be a breach, but have not yet gotten a response.

Again, it's not clear to me whether this latter incident should have been reported to HHS, as pre-HITECH, there was no obligation to notify HHS or individuals, although as HHS reminded me today, there was an obligation to mitigate any harm and to have a security incident response plan. But as of right now, we don't even know when LabMD first learned of the data theft (if that's what it was), so it's hard to figure out which laws even applied on a federal level, much less a state level. If they first learned of it after September 23, 2009, then HITECH provisions should apply.

I'll try to update this post if I can get more details.

Meanwhile, over on DataBreaches.net, I've posted the portion of the complaint that addresses [LabMD's alleged security failures](#), as it provides some guidance to businesses (and HIPAA-covered entities) about what practices may run you afoul of the FTC Act.

Posted by Dissent at 8:32 pm

Tagged with: LabMD

Sorry, the comment form is closed at this time.

Featured Articles

NY: Martin Luther King Jr. Health Center learns of subcontractor's breach four years later, responds to breach admirably

Lanap and Implant Center patients never told that their Social Security numbers were – and are – still online for download?!

Commentary: Shooting the Messenger is Not an Effective Incident Response Strategy (updated)

Thousands of Pennsylvania dental patients may be at lifetime risk of ID theft after patient database is uploaded to torrent sites

San Francisco Doctor Accepts Bitcoin to Protect Patient Privacy

Recent Posts

iPharmacy app gets negative review from Apphority

Calgary pharmacist used private health information to hit on patient: report Vermont health official reports 2nd breach involving state health insurance exchange

Assessing Bitcoin's benefits, security risks in healthcare

Psychological assessments provider notifies patients after laptop with PHI stolen in office burglary

Two laptops with PHI stolen from UHS-Pruitt employees' cars in a two-week period

Colorado Health & Wellness notifies patients after doctor who left practice took their contact information with him

NY: Martin Luther King Jr. Health Center learns of subcontractor's breach four years later, responds to breach admirably

Texas orthopedic group notifies patients after desktop computers were stolen in burglary

Update to HHS's breach list (update 1)

Recent Comments

Dissent on San Francisco Doctor Accepts Bitcoin to Protect Patient Privacy

Ryan on San Francisco Doctor Accepts Bitcoin to Protect Patient Privacy

Dissent on Commentary: Shooting the Messenger is Not an Effective Incident Response Strategy (updated)

Kaiser Permanente notifies members after e-mail attachment error

Errant e-mail creates security breach at MNSure

FTC Blasts LabMD's Bid To Stall Data Security Suit

By **Allison Grande**

0 Comments

Share us on:

Law360, New York (December 06, 2013, 7:03 PM ET) -- The Federal Trade Commission on Thursday shot back at claims that its data security suit against LabMD Inc. should be paused while the company challenges the regulator's allegations in the 11th Circuit and District of Columbia, saying the delay would undermine the commission's adjudicative processes.

Since the commission filed its administrative complaint against LabMD in August, the medical testing laboratory has rallied against the assertion that the FTC has the authority to regulate the security of patient information as an "unfair" practice under Section 5 of...

To view the full article, take a free trial now.

Try Law360 FREE for seven days

Already a subscriber? [Click here to login](#)

Sections

Health

Privacy

Law Firms Mentioned

Dinsmore & Shohl

Government Agencies Mentioned

Federal Trade Commission

Related Articles

FTC Rejects LabMD's Bid To Halt Data Security Suit

FTC Sues To Get Patient Data Spreadsheet From LabMD

LabMD Slams 'Oppressive' FTC Subpoenas In Data Breach Row

LabMD Unleashes Trump Card In FTC Data Security Fight

FTC's Increasingly Aggressive Assertion Of Authority

[★ BOOKMARK THIS SITE](#)
[🔍 SEARCH](#)

[GO](#)
[🛒 DOWNLOAD BASKET](#)
[🌐](#)
[📺](#)
[t](#)
[f](#)
[YOUR ACCOUNT](#)



TODAY'S NEWS: [State of Former Soviet Croplands Still Undecided](#)

[🏠](#)
[WINDOWS](#)
[GAMES](#)
[DRIVERS](#)
[MAC](#)
[LINUX](#)
[SCRIPTS](#)
[MOBILE](#)
[HANDHELD](#)
[NEWS](#)

NEWS CATEGORIES:

Home > News > Security

- Latest News
- Oddiverse
- NEW! Laptops & Tablets
- NEW! 3D Printing
- NEW! Photo
- Games
- Microsoft
- Apple
- Telecoms
- Technology & Gadgets
- Reviews
- Linux
- Life and Style
- Webmaster
- Security
- Editorials
- Interviews
- Science
- Green

August 30th, 2013, 08:41 GMT · By [Eduard Kovacs](#)

FTC Accuses Medical Testing Lab LabMD of Exposing Details of 10,000 People

PC Checkup - Free Trial

computercheckup.aol.com

Computer Checkup helps speed up and de-junk your slow PC. Try it free!

SHARE: [+1](#) 2

Like Share 0

Tweet 7

Adjust text size: - +



The US Federal Trade Commission (FTC) has filed a complaint against LabMD, Inc., an Atlanta-based medical testing lab. The FTC alleges that the company has exposed the personal information of close to 10,000 people.

According to the agency, the LabMD billing information of over 9,000 individuals was posted on a peer-to-peer file-sharing network. The data included social security numbers, names, dates of birth, insurance info, and [medical treatment](#) codes.

[ENLARGE](#)

[NEWS ARCHIVE >>](#)
[SOFTPEDIA REVIEWS >>](#)
[MEET THE EDITORS >>](#)

I ❤️ SOFTPEDIA

[+1](#) 41k

[+](#) Find us on Google+

Like 186k

Follow @softpedia

Softpedia

TRENDING TODAY

- Download UC Browser 9.3 for Java
- Ubuntu Might Replace Windows XP in South Korea
- Steam Winter Sale 2013 Gets Teased by Valve with Snow Globe Trading Cards
- United Nations Approves Internet Privacy Resolution
- Download UC Browser 9.2 for Java
- Download BBM for Android 1.0.2.83
- New Ubuntu 14.04 Icons Are Drop-Dead Gorgeous, Might Not Arrive in Desktop Version
- The Pirate Bay Gets Kicked Out of Peru, Moves to Guyana Domain
- WhatsApp Messenger 2.11.340 Arrives on Windows Phone
- Opera Max for Android Is More Than a Browser, Out Now on Google Play

In addition, in 2012, the personal [information](#) of at least 500 individuals was found in the possession of identity thieves. At the time, police found documents containing names, social security numbers and, in some cases, even bank account information.

"The unauthorized exposure of consumers' personal [data](#) puts them at risk," said Jessica Rich, Director of the FTC's Bureau of Consumer [Protection](#).

"The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate [security](#) measures to prevent it from falling into the hands of identity thieves and other unauthorized users."

On the other hand, LabMD representatives deny the accusations.

In a statement sent to [Ars Technica](#), the company's representatives noted, "The Federal Trade Commission's enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority to engage in an ongoing witch hunt against private [businesses](#)."

"The allegations in the FTC's complaint are just that: allegations. LabMD looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes," the statement continues.

"The FTC has repeatedly overstepped its statutory authority under Section 5 of the Federal Trade Commission Act and the FTC does not have the authority to bring this enforcement [action](#)."

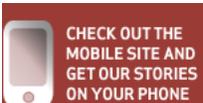
Follow @EduardKovacs 4,538 followers

FILED UNDER: [FTC](#) [DATA BREACH](#) [CONTROVERSY](#) [DATA LEAK](#) [IDENTITY THEFT](#)

1st Social Knowledge Base

mindtouch.com/Social_Knowledge_Base

w/ Support Ticket Integration, Real Time Search, Drag/Drop & Reporting!



Share your thoughts on this story...



Ensuring YOU control your sensitive health information

SEARCH

- Home
- Who We Are
- What We Do
- How You Can Help
- Summit
- Blog
- Events

FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy

By Deborah Peel | August 29, 2013 | Tagged With: [data mining](#), [data security](#), [Data Theft/Breach](#), [EHR](#), [EHRs](#), [electronic medical records](#), [health it](#), [LabMD](#), [security](#), [technology](#) | [Leave a Comment](#)

The public would be surprised how little thought or money healthcare businesses put into data security. LabMD is probably just one of thousands of healthcare businesses that don't encrypt patient data and whose employees who use file-sharing apps to download music, etc, exposing patient records online.

We need new laws that require businesses that hold health data to be audited to prove they protect it.

Shouldn't businesses have to prove they use tough data security protections before they are allowed to handle sensitive health information?

To view the full article, please visit: <http://www.ftc.gov/opa/2013/08/labmd.shtm>

Share this:

Like 0

Tweet 0

Share

Print

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

1



Like

2



Tweet



North Carolina Consumers Council

- [home](#)
- [about](#)
- [membership](#)
- [news & info](#)
- [contact](#)
- [discounts](#)

FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy

The [Federal Trade Commission \(FTC\)](#) has filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers.

The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data.

LabMD conducts laboratory tests on samples that physicians obtain from consumers and then provide to the company for testing. The company, which is based in Atlanta, performs medical testing for consumers around the country. The Commission's complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data – including health information – it held.

The complaint alleges that a LabMD spreadsheet containing insurance billing information was found on a P2P network. The spreadsheet contained sensitive personal information for more than 9,000 consumers, including names, Social Security numbers, dates of birth, health insurance provider information, and standardized medical treatment codes. Misuse of such



insurance provider information, and standardized medical treatment codes. Misuse of such information can lead to identity theft and medical identity theft, and can also harm consumers by revealing private medical information.

The complaint also alleges that in 2012 the Sacramento, California Police Department found LabMD documents in the possession of identity thieves. These documents contained personal information, including names, Social Security numbers, and in some instances, bank account information, of at least 500 consumers. The complaint alleges that a number of these Social Security numbers are being or have been used by more than one person with different names, which may be an indicator of identity theft.

The complaint includes a proposed order against LabMD that would prevent future violations of law by requiring the company to implement a comprehensive information security program, and have that program evaluated every two years by an independent, certified security professional for the next 20 years.

The order would also require the company to provide notice to consumers whose information LabMD has reason to believe was or could have been accessible to unauthorized persons and to consumers' health insurance companies.

Posted: Friday, August 30, 2013



[North Carolina Attorney General's Office: Consumer Protection Division](#) | [National Do Not Call Registry](#) | [Federal Trade Commission](#) | [Consumer Financial Protection Bureau](#)
[Consumer Product Safety Commission](#) | [National Highway Traffic Safety Administration](#) | [Food & Drug Administration](#) | [Consumer Reports](#)

[North Carolina Consumers Council, Inc](#) © 2013 • [Privacy Policy](#) •

NCCC is a nonprofit, nonpartisan consumer organization promoting consumer awareness, consumer education and consumer protection both within North Carolina and beyond our borders. We assist consumers with complaints, credit union membership, general advice, money-saving tips, scam alerts, recall notices, lawyer referrals, member discounts and more.



- **PHI DEFINED**
- **CHALLENGES**
- **SOLUTIONS**
- **RESOURCES**
-

The FTC claims an Atlanta medical lab didn't do enough to protect its records, resulting in the leak of SSNs of 9,000 consumers

September 5, 2013

By ANNE FLAHERTY
Associated Press

WASHINGTON (AP) – The Federal Trade Commission on Thursday accused a small Atlanta-based medical lab that specializes in cancer detection of not doing enough to protect its patients' online records, resulting in the leak of Social Security numbers and birth dates of more than 9,000 consumers.

The complaint against LabMD describes what many consumers fear: being forced to hand over personal information to a doctor's office or hospital, not knowing how that data is handled or who has access to it, only to become vulnerable to identity theft. The allegations also raise questions about the federal government's push for the health care industry to swap paper for electronic records to save money when doing so relies on cybersecurity investments by private companies.

In a statement, LabMD said the company "looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes."

Jessica Rich, director of the FTC's bureau of consumer protection, said LabMD's practices put consumers at serious risk of identity theft.

"The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users," she said in a statement.

More than half of doctors' offices and 4 out of 5 hospitals have transitioned from paper to electronic medical records, according to the government. Moving to computerized records is the rare consensus issue in health care, enjoying support from across the political spectrum. Taxpayers have already contributed more than \$14 billion to help speed the move through an incentive program that was part of the Obama administration's economic stimulus package.

The hope was that going digital would make caring for patients safer and less costly by helping avoid medical mistakes and cutting down on duplicative tests. But concerns have also surfaced about patient privacy and vulnerability to fraud. And progress has been mixed in getting medical computers from different offices to talk to each other, the key to a seamlessly efficient system.

A pair of reports in 2011 by the Health and Human Services inspector general warned that the drive to connect hospitals and doctors electronically was being layered on top of a system that already has privacy problems. The administration said in response it would pursue stronger safeguards.

The complaint filed Thursday means that the allegations will be tried in a formal hearing before an administrative law judge. The FTC wants the judge to order LabMD to institute a comprehensive information security program with professional audits every two years for the next 20 years. The proposed order also would require LabMD to notify consumers whose information was compromised.

LabMD founder Michael Daugherty has objected to these terms and has been fighting the FTC investigation for several years. He claims on his personal website that LabMD is a victim of theft by a cybersecurity firm that he says was trying to sell his company services. Daugherty says that when he refused, the stolen data was supplied to government regulators, who are using the leak to punish him as a small business owner and justify additional government regulation. Daugherty has written a book on the subject that he says will be published in September.

The trade commission's "enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority to engage in an ongoing witch hunt against private businesses," LabMD said in its statement.

According to the FTC complaint, a LabMD spreadsheet with insurance billing data on more than 9,000 consumers was discovered on a public file-sharing network. The spreadsheet contained Social Security numbers, birth dates, insurance information and medical treatment codes. The FTC says California police later discovered that identity thieves had acquired personal data from at least 500 LabMD consumers.

In its complaint, the FTC said lax security controls at LabMD resulted in the leak of the spreadsheet. Regulators say the company did not maintain a "comprehensive data security program" or use "readily available measures" to identify common vulnerabilities. The company also did not adequately train employees or prevent unauthorized access, according to the FTC.