- How should businesses relay key information about their privacy practices to consumers, including how they may be collecting, using, or sharing consumer data?

The Commission is devoting significant resources to addressing the mobile phenomena: in addition to setting up a dedicated Mobile Technology Unit of tech-savvy folks, we have held workshops on Mobile Privacy Disclosures, Mobile Cramming, and Mobile Apps for Kids.[14] Last June, the FTC hosted a public forum entitled *Mobile Security: Potential Threats and Solutions*, which brought together researchers, technologists, and industry participants from across the mobile ecosystem to discuss a variety of mobile security issues, including the threat posed by the rise of mobile malware.[15] We have also issued reports, conducted research, and developed extensive consumer and business education materials.

We have also been active on the enforcement front, bringing two mobile cramming cases resulting from companies placing unauthorized charges on phone bills, which will lead to refunds for consumers.[16] We have many more cases in the mobile area in the pipeline.

Market Developments

Aside from focusing solely on government activities, an important question that I will continue to focus on in 2014 is whether the privacy options consumers desire are available to them through products or services in the marketplace or through industry self-regulation.

Many companies are now developing products that cater directly to consumers with heightened privacy preferences. For example, the extensibility of the modern browser allows developers to incorporate privacy protections into consumers' everyday browsing. A wide range of privacy and security protection add-ons are available for all of the major Internet browsers. One such add-on, Ghostery, helps users easily detect tools that behavioral advertisers often use to track individuals across sites.[17] Identifying these tools promotes transparency by giving consumers more information on the advertising practices of the sites that they visit regularly.

---

[14] Press Release, Fed. Trade Com'n, FTC Announces Final Agenda and Panelists for Workshop about Advertising and Privacy Disclosures in Online and Mobile Media (May 28, 2012), *available at* http://ftc.gov/opa/2012/05/dotcomdiscl_ma.shtm; Press Release, Fed. Trade Com'n, FTC to Host Mobile Cramming Roundtable May 8 (Mar. 8, 2013), *available at* http://www.ftc.gov/opa/2013/03/mobilecramming.shtm; Press Release, Fed. Trade Com'n, FTC's Second Kids' App Report Finds Little Progress in Addressing Privacy Concerns Surrounding Mobile Applications for Children (Dec. 10, 2012), *available at* http://www.ftc.gov/opa/2012/12/kidsapp.shtm.

[15] Press Release, Fed. Trade Com'n, FTC Announces Agenda, Panelists for Upcoming Mobile Security Forum (May 24, 2012), *available at* http://ftc.gov/opa/2013/05/mobilethreats.shtm.

[16] Press Release, Fed. Trade Com'n, FTC Files Its First Case Against Mobile Phone "Cramming" (April 17, 2013), *available at* http://www.ftc.gov/opa/2013/04/wisemedia.shtm; Press Release, Fed. Trade Com'n, Jesta Digital Settles FTC Complaint it Crammed Charges on Consumers Mobile Bills Through 'Scareware' and Misuse of Novel Billing Method (Aug. 21, 2013), *available at* http://www.ftc.gov/opa/2013/08/jesta.shtm.

[17] http://www.ghostery.com/.

Self-regulation can also offer consumers more privacy choices. The best self-regulatory programs are nimble, keeping pace with rapid changes in technology and business practices in ways legislation and regulation cannot. A good example of a self-regulatory program is the Network Advertising Initiative (NAI), which this year released an updated Code of Conduct and a new Mobile Application Code, which for the first time addresses the collection and use of data from mobile apps.[18] Another example of self-regulation is the Digital Advertising Alliance (DAA), which has developed a notice and choice mechanism through a standard icon in ads and on publisher sites, deployed the icon broadly, obtained commitments from the vast majority of the behavioral advertising market, and established an enforcement mechanism to ensure compliance.

Conclusion

I hope that I have reassured you that the U.S. does care deeply about consumer privacy. Through the FTC's enforcement, education and policy work, we are able to provide strong privacy protections to American consumers. This important work will continue to be a top priority for the agency in 2014 and beyond.

Thank you for the opportunity to address you today. I look forward to our discussion.

---

[18] Network Advertising Initiative, 2013 NAI Code of Conduct, *available at* http://www.networkadvertising.org/sites/default/files/2013_nai_code_pr.pdf; Network Advertising Initiative, 2013 NAI Mobile Application Code, *available at* http://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf.

Remarks of FTC Commissioner Maureen K. Ohlhausen
Google Data Security Event
Washington, D.C.
April 17, 2013

Thank you so much for your kind introduction. I appreciate the invitation to discuss one of the most important and timely topics in the consumer protection area—data security. This is a core issue for the Federal Trade Commission and I would like to share with you our role in regulating it. Let me preface my remarks by saying that my comments are my own and do not necessarily reflect those of my colleagues on the Commission.

Data is an increasingly vital asset, and as companies collect more and more personal information from their customers, they need to protect this information from theft and unauthorized access, which can hurt customers and harm the business' reputation. That's where data security comes in. Data security is part of the broader topic of data privacy, which encompasses the use of consumer data by a wide variety of entities, with which the consumer often (but not always) has willingly shared information, for a wide variety of purposes. Data security, which I will focus on today, examines how entities safeguard the consumer data that they maintain from unauthorized access by data hackers or from insiders without a legitimate need for that information. Regardless of how one feels about the use of consumer data for marketing or targeting purposes, I believe we can all agree that failing to take reasonable precautions to secure data from identity thieves and other malicious parties hurts consumers and legitimate businesses alike.

As with most issues, the FTC approaches its role in data security on several fronts: law enforcement, policy and research, and business/consumer education. This multi-prong approach allows the agency to maximize its impact by challenging the actions of wrong-doers, educating consumers on how to protect themselves and their data, and sharing practical tips and best practices with businesses to help them keep their consumer data secure.

I will begin by sharing with you a bit about the FTC's enforcement record and the types of cases we bring in the data security arena. Next, I will discuss the excellent materials we offer to consumers and businesses alike on data security. Then, I will offer some practical guidance on how businesses can best protect the data entrusted to them. Finally, I will make a few observations on where we are going with new technologies, such as mobile and facial recognition, that are creating new challenges in the data security landscape for both the FTC and Congress.

Enforcement

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security. The Commission enforces several laws and rules that impose obligations upon businesses that possess consumer data. The Commission's Safeguards Rule[1] under the Gramm-Leach-Bliley Act (GLB)[2], for example, imposes data security requirements on financial institutions. The Fair Credit Reporting Act (FCRA) requires credit reporting agencies to use reasonable procedures to ensure that recipients of sensitive consumer information have a permissible purpose for receiving that information from the agencies.[3] It also imposes safe disposal obligations on entities that maintain consumer report information.

---

[1] FTC Safeguards Rule, 16 C.F.R. § 314 (2013).
[2] The Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).
[3] The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006).

Additionally, we enforce Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer harm.[4] Under these statutes, we have initiated over three dozen data security cases.

In January, the Commission brought a case against Cbr, a leading cord blood bank, for failing to protect nearly 300,000 customers' personal information, including Social Security numbers, credit and debit card account numbers, and sensitive medical information.[5] The breach occurred when unencrypted back-up files and a laptop were stolen from a backpack left in an employee's car for several days. We also settled additional charges that Cbr failed to take sufficient measures to prevent, detect, and investigate unauthorized access to computer networks.

Last June, the FTC filed a complaint against Wyndham Hotels for failure to protect consumers' personal information, resulting in three data breaches in less than two years.[6] According to the FTC's complaint, Wyndham and its subsidiaries failed to take security measures, such as using complex user IDs and passwords and deploying firewalls and network segmentation between the hotels and the corporate network. In addition, Wyndham allegedly permitted improper software configurations that resulted in the storage of sensitive payment card information in clear readable text. The complaint alleges that these failures resulted in fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' account information to an Internet domain address registered in Russia. A central allegation of the Commission's case is that Wyndham's privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information and that its failure to safeguard personal information caused substantial consumer injury. This case is currently in active litigation.

Data Broker Study

Another important tool used by the Commission is policy research, which helps us keep abreast of new business models that use consumer data and aids our understanding of how innovations may affect data security and consumer privacy. In this context, the Commission recently began a study of the data broker industry.[7] We sent out formal requests for information to nine large data brokers to learn more about their practices, including how they use, share, and secure consumer data. It is vital that we have a good understanding of data usage by brokers because appropriate use of data can greatly benefit consumers through better services and increased convenience, while inappropriate use or insecure maintenance of data could cause significant harm to consumers. We will carefully analyze the submissions from the companies and use the information to decide how to proceed in this area. Congress is also taking a closer look at this industry, so I expect it will be a hot topic of discussion in the data privacy and security community in the days ahead.

---

[4] 15 U.S.C. § 45.

[5] Press Release, Fed. Trade Com'n, Cord Blood Bank Settles FTC Charges that it Failed to Protect Consumers' Sensitive Personal Information (Jan. 28, 2013), *available at* http://www.ftc.gov/opa/2013/01/cbr.shtm.

[6] Complaint, FTC v. Wyndham Worldwide Corporation, et al. (D. Ariz. 2012) (No. 12 Civ. 1365).

[7] Press Release, Fed. Trade Com'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://ftc.gov/opa/2012/12/databrokers.shtm.

Consumer and Business Education

The Commission also promotes improved data security practices through extensive use of consumer and business education. On June 4, the FTC is sponsoring a public forum to address security threats facing users of smartphones and other mobile technology. This session will provide an opportunity for the Commission's staff to learn more about data security challenges facing consumers and businesses, as well as educate the public on how to secure and protect their data.

One of the most effective ways the FTC supports data security is through OnGuardOnline.gov, a website designed to educate consumers about basic computer security. Since its launch in 2005, the site has received nearly 20 million visits.

In addition, the Commission engages in wide-ranging efforts to educate consumers on the issue of identity theft, one of the serious, potential consequences of a data breach. Our efforts focus on providing consumers with practical tips on how to protect their identities, as well as steps to take if they have already become victims of identity theft. The FTC's identity theft primer and victim recovery guide have been distributed to millions of consumers in print and online, and every week around 20,000 consumers contact our identity theft hotline and website dedicated to helping victims.

The FTC provides outreach to businesses as well. Our business guide on data security, along with an online tutorial, has been widely disseminated.[8] It is designed to offer practical and concrete advice to businesses—especially small businesses—on how to develop and implement data security plans. We have developed other materials specifically for business through the BCP Business Center, which has a section dedicated to helping businesses learn best practices to protect sensitive data in their possession.[9]

Better Data Security Practices for Businesses

The saying is that an ounce of prevention is worth a pound of cure, so we strive to provide guidance to businesses on better data security practices. So, what are the basic steps that businesses can take to minimize the risk of a data breach or security compromise? Much of it is just common sense. First, businesses should build in privacy and security considerations from the start, a concept we call "privacy by design." This phrase means incorporating privacy protections into the development of a business plan or product. Other steps include limiting information collected to what is necessary for business operations, securely storing collected data, and safely disposing of data that is no longer needed. These steps seem so simple, yet many of the data security cases brought by the Commission involve companies who engaged in careless practices, such as dumping sensitive medical or financial records into open trash bins or failing to take basic steps to secure computer networks.

It is critical that businesses honor the promises they make to protect consumers' privacy. This concern is at the heart of the Commission's law enforcement against deceptive practices. Businesses must live up to the assurances they make regarding security standards.

---

[8] FED. TRADE COM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), *available at* http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf; Online Tutorial, Fed. Trade Com'n, Protecting Personal Information: A Guide for Business (2011), http://business.ftc.gov/multimedia/videos/protecting-personal-information.

[9] FED. TRADE COM'N, http://business.ftc.gov/privacy-and-security/data-security (last visited Apr. 17, 2013).

Because breaches may still occur even in the most security-conscious companies, however, it is also critical to have a plan for responding to data breaches before they happen. Putting together a response plan now may help reduce the impact of a data breach on a business and its customers later.

Data Security with New Technologies

As we look to the future, new technologies and business models bring great benefits to consumers but also new data security challenges. In the Commission's 2010 case against social networking service Twitter, the FTC charged that lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter.[10] As a result, hackers had access to private "tweets" and non-public user information – including users' mobile phone numbers – and took over user accounts. The Commission's order, which applies to Twitter's collection and use of consumer data through mobile devices or applications, prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.[11]

Facial recognition is another cutting-edge technology offering both great benefits and potential risks in the area of data security. This technology can identify a specific face by evaluating and comparing unique biometric data from facial images. This technology can benefit consumers by, for example, allowing a mobile phone user to use her face, rather than a password, to unlock her phone. Millions of consumers already enjoy one of the most prevalent current uses of this technology, which enables semi-automated photo tagging or photo organization on social networks and in photo management applications. On the other hand, facial recognition technology also creates particular data security risks because a face is a unique identifier that, unlike a credit card number or ID number, cannot be changed easily if the biometric data is compromised.

Data Security Legislation

Speaking of faces, some familiar faces from past privacy and data security legislative efforts are absent in the 113th Congress, and it is not yet clear how this will affect the discussion. In the last Congress, there was strong, bipartisan support for data security legislation. One effort that had bipartisan support in the past Congress was a federal breach notification and data security law. There is some ongoing discussion about including this as part of a cybersecurity bill. The theory is that combining two important—and somewhat related—measures would increase the likelihood of passage.

Although the FTC can proceed using its Section 5 authority—and since 2001 has brought almost forty cases against companies for failing to protect consumer information—there are gaps that could be closed through carefully crafted federal legislation. Currently, almost all states have data security laws on the books that require consumer notification if personal information has been compromised. Although some of the laws are similar, they are not identical. This lack of uniformity in the laws means that companies must comply with all of the different state notice requirements, and consumers may get notifications that are substantively different and are triggered by different types of breaches. A single standard would create uniform procedures within companies and would clarify consumer expectations. I believe that, if carefully crafted, such a law is likely to benefit both consumers and business, particularly because, unlike uses of consumer information for advertising, product improvement, or fraud reduction,

[10] Complaint, In re Twitter, Inc., No. 092-3093, (F.T.C. June 24, 2010), http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf.

[11] Decision and Order, In re Twitter, Inc., No. 092-3093, (F.T.C. Mar. 2, 2011), http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.

there are no benefits to consumers or competition from allowing consumer data to be stolen. At the same time, any such law would have to carefully consider what are reasonable precautions for safeguarding various types of data without imposing undue costs that are not justified by consumer benefits.

Thank you for inviting me to speak with you. I am happy to take questions.

EXHIBIT

31

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

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

OPPOSITION TO MOTIONS TO QUASH AND FOR PROTECTIVE ORDER REGARDING SUBPOENAS SERVED ON SCOTT MOULTON AND FORENSIC STRATEGY SERVICES, LLC

INTRODUCTION

Complaint Counsel submits this opposition to the Motions to Quash and for Protective Order filed by LabMD, Scott Moulton, and Forensic Strategy Services, LLC ("Forensic") regarding Complaint Counsel's subpoenas to Scott Moulton and Forensic. Because the motions of LabMD, Inc. ("LabMD"), Moulton, and Forensic present largely identical arguments, Complaint Counsel hereby submits this consolidated response for the Court's convenience.

This Court should deny the Motions to Quash and for Protective Order because they seek to shield from discovery facts that bear on the allegations of the Complaint, the proposed relief, and LabMD's anticipated defenses. To the extent that any attorney work product immunity from discovery may apply, neither Respondent nor Moulton nor Forensic have made the requisite showing by producing a privilege log. Relatedly, Complaint Counsel is entitled to discovery of the facts underlying and asserted in a public affidavit used by LabMD in litigation.

Further, LabMD's and Moulton's respective motions are untimely. Finally, a confidentiality provision in a private contract – that in any event excludes information made

public by LabMD – is not a legitimate basis for resisting information sought in a government subpoena.

BACKGROUND

The Complaint alleges that LabMD engaged in unfair practices in violation of Section 5 of the FTC Act by failing to take reasonable and appropriate measures to prevent unauthorized access to consumers' personal information. Compl. ¶¶ 6-11, 17-21. One of the results of LabMD's failures is that a LabMD file containing the sensitive personal information of approximately 9,300 consumers ("the P2P insurance aging file") was shared to a public peer-to-peer ("P2P") file sharing network without being detected by LabMD. *Id.* ¶¶ 10(g), 17-20.

As a preliminary matter, LabMD incorrectly assumes that this action relates only to LabMD's exposure of sensitive consumer data over P2P networks. In fact, the Complaint alleges that LabMD's overall data security practices were woefully inadequate, creating potential exposure of consumer data on many fronts. See Compl. ¶ 10 (outlining several deficiencies in LabMD's data security practices). The exposure of names, dates of birth, Social Security numbers, codes for lab tests conducted, health insurance company names, addresses, and policy numbers to the public over the P2P network is a prime example and a devastating consequence of LabMD's lax data security.

In May 2008, Tiversa, Inc. ("Tiversa") informed LabMD that the file LabMD exposed was available on a public file sharing network. *Id.* ¶ 17. LabMD subsequently filed suit in Georgia state court against Tiversa, asserting a variety of claims related to Tiversa obtaining the P2P insurance aging file. *LabMD, Inc. v. Tiversa, Inc.*, No. 11-cv-04044 (N.D. Ga. Nov. 23, 2011). The case was removed to federal court, and Tiversa filed a motion to dismiss.

In LabMD's response to Tiversa's motion to dismiss, LabMD attached an affidavit from Scott Moulton, an IT provider it retained. *See* Affidavit of Scott A. Moulton, *LabMD, Inc. v. Tiversa, Inc.*, No. 11-cv-04044 (N.D. Ga. Jan. 13, 2012), ECF No. 16-1 (attached as Exhibit A). Moulton is the President of and Lead Certified Computer Forensic Specialist for Forensic. *See id.* Moulton's affidavit, as outlined below, includes facts that bear directly on the Complaint's allegations, the proposed relief, and LabMD's anticipated defenses, including: the P2P insurance aging file, which the affidavit refers to as the "May 13 file"; LabMD's contention that Tiversa stole the P2P insurance aging file by opening a physical TCP/IP connection on LabMD's computer[1]; and the availability of the P2P insurance aging file on computers outside of LabMD.[2] *Id.* ¶¶ 5-15.

Indeed, as part of its defense in this matter, LabMD has asserted that the P2P insurance aging file was stolen from LabMD through a hack of its network. *See, e.g.*, Transcript of Initial Scheduling Conference at 24, Statement of Reed Rubinstein, Cousel for LabMD, Inc., In the Matter of LabMD, Inc., FTC Docket No. 9357 (Sept. 25, 2013) ("And actually, I would like to if

---

[1] Complaint Counsel intends to show that LabMD is simply wrong that Tiversa accessed LabMD's network to obtain the insurance aging file. Instead, the evidence will show that Tiversa obtained the file not from LabMD but from the computers of parties not related to LabMD.

[2] Moulton's work for LabMD also is chronicled in *The Devil Inside the Beltway*, a book published by LabMD's CEO, Michael Daugherty. Michael J. Daugherty, *THE DEVIL INSIDE THE BELTWAY* 329, 332-33 (Broadland Press 2013).

I could, just take issue with the file that triggered this investigation was not shared; it was stolen. A company called Tiversa . . . .").[3]

Based on Moulton's affidavit in the Tiversa case, Complaint Counsel issued subpoenas to Moulton and Forensic on October 24, 2013.[4] Moulton and Forensic did not move to quash Complaint Counsel's subpoenas in the time period prescribed by Rule 3.34(c), which elapsed on November 6, 2013. 16 C.F.R. § 3.34(c).

On November 5, 2013, LabMD filed a Motion for a Protective Order that sought to prevent Complaint Counsel from engaging in third party discovery, specifically naming Moulton and Forensic. *See* Respondent LabMD, Inc.'s Motion for a Protective Order at 2 n.1, In the Matter of LabMD, Inc., Docket No. 9357 (Nov. 5, 2013). At no point did LabMD raise in its November 5, 2013 Motion any of the arguments it now asserts with respect to Moulton and Forensic. *Id.*

On November 21, 2013, the deadline for Moulton and Forensic to produce documents, Complaint Counsel received a letter from Moulton, dated November 19, 2013, outlining objections to Complaint Counsel's document subpoenas.[5] *See* Letter from Scott Moulton, Forensic Strategy Services, LLC to Matthew Smith, Paralegal, Federal Trade Commission (Nov. 19, 2013) (attached as Exhibit B) ("November 19 letter").

---

[3] LabMD further put the subject of Moulton's affidavit at issue in this matter by questioning Robert Boback, the CEO of Tiversa, in a November 2013 deposition regarding Tiversa's acquisition of the P2P insurance aging file.

[4] LabMD (Resp. Motion at 1) and Forensic's (Forensic Motion at 1) assertion that Complaint Counsel served a deposition subpoena on Forensic is mistaken. It served a deposition subpoena on Moulton, and document subpoenas on Moulton and Forensic.

[5] At that time, Moulton and Forensic were not represented by counsel in this matter.

Upon receipt of the November 19 letter, Complaint Counsel called Moulton. During this call, Moulton agreed to be deposed on February 6, 2014 but stated that he would refuse to answer any questions about LabMD, citing attorney work product. Complaint Counsel re-served Moulton on November 27, 2013 for his February 6, 2014 deposition.

On December 6, 2013, Complaint Counsel spoke by phone with LabMD's counsel regarding the subpoenas to Moulton and Forensic. LabMD's counsel requested that Complaint Counsel withdraw its subpoenas and stated that it would move to quash the subpoenas and seek a protective order if Complaint Counsel did not withdraw them.

On December 9, 2013, Complaint Counsel spoke with counsel retained by Moulton and Forensic, who likewise requested that Complaint Counsel withdraw its subpoenas and indicated that it otherwise would move to quash the subpoenas and seek a protective order. At no point during the December 6, 2013 or December 9, 2013 calls did LabMD's counsel or Moulton and Forensic's counsel state that they considered Moulton an expert consultant; nor did they reveal LabMD's intentions about not designating Moulton as an expert in this matter. Although their motions invoke the attorney work product doctrine, Moulton and Forensic have not to date provided Complaint Counsel with a privilege log, as requested in the document subpoenas and as required under Rule 3.38(A). 16 C.F.R. § 3.38A.

ARGUMENT

I. COMPLAINT COUNSEL'S SUBPOENAS TO MOULTON AND FORENSIC ARE REASONABLY EXPECTED TO YIELD INFORMATION RELEVANT TO ALLEGATIONS OF THE COMPLAINT, PROPOSED RELIEF, OR DEFENSES IN THIS ACTION

Complaint Counsel's subpoenas seek discovery "reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses

of any respondent." 16 C.F.R. § 3.31(c)(1). The facts Moulton asserts in his publicly filed sworn affidavit and that also appear in a published book relate directly to the Commission's allegations. These facts also were put at issue by LabMD in this litigation and therefore relate to LabMD's defenses. *See, e.g.,* Transcript of Initial Scheduling Conference at 24, Statement of Reed Rubinstein (Sept. 25, 2013).

For example, Moulton states in his affidavit that he examined the computer file Tiversa presented to LabMD and the file has a unique SHA-1 value.[6] *See* Affidavit of Scott A. Moulton ¶ 13. Moulton also states that he has not found any evidence that the file Tiversa presented to LabMD exists on any computer other than the LabMD computer where the file was saved. *Id.* ¶ 15. These facts are directly relevant to the Complaint's allegations regarding the reasonableness of LabMD's data security practices and the P2P file sharing incident, as well as LabMD's defenses about the widespread availability of the insurance aging file, Compl. ¶¶ 10, 13-20. Therefore, LabMD's contention that the documents and testimony sought from Moulton, particularly the facts in Moulton's affidavit and the facts supporting it, lack relevance to this action is without merit.

LabMD engaged Moulton and his company to examine the insurance aging file, analyze its metadata, and search P2P networks for the file. LabMD then publicly disclosed Moulton's work and the results of it in a court-filed affidavit and a publicly available book. Having done so, LabMD cannot now seek to hide Moulton's work, the methods and techniques he used, and the results of his investigation. Each is highly relevant to the claims at issue in this action, as well as defenses raised by LabMD in this action.

---

[6] An SHA-1 value is a unique signature associated with the file.

II. LABMD WAIVED THE ATTORNEY WORK PRODUCT DOCTRINE AS TO MOULTON'S AFFIDAVIT AND THE FACTS UNDERLYING IT AND CANNOT HIDE BY LABELING MOULTON AN EXPERT CONSULTANT

In evaluating LabMD's work product claim,[7] this Court should find that LabMD waived it with respect to Moulton's affidavit and the facts underyling it.[8] Facts put forth by LabMD to support its defense are included in Moulton's public affidavit and disclosed in Daugherty's book. Because LabMD publicly disclosed Moulton's affidavit and has squarely raised as a defense *in this litigation* the circumstances under which Tiversa came into possession of the P2P insurance aging file, it is appropriate for Complaint Counsel to seek discovery on these issues. *See* 8 CHARLES ALAN WRIGHT ET AL., Federal Practice and Procedure, §§ 2016.4, 2016.6 (3d ed. Apr. 2013) (explaining work product protection is waived when holder of protection puts protected material at issue).

LabMD (as well as Moulton and Forensic) cannot now attempt to frustrate discovery by labeling Moulton an expert consultant. Complaint Counsel should be permitted to obtain documents that Moulton relied upon when preparing his affidavit as well as question Moulton about the facts in his affidavit and the facts underyling it. Further, like Moulton and Forensic, LabMD has not to date provided Complaint Counsel with a privilege log or even a description of the documents subject to the protection invoked in its motion, and the Court should order one to

---

[7] It is well-established that to the extent that the attorney work product may be applicable here, it does not belong to Moulton and Forensic. *See In re OSF Healthcare Sys.*, No. 9349, 2012 WL 1355596, at *1 n.2 (noting that work product does not belong to third party consultant retained by Respondents but to Respondents directly); *In re Grand Jury Subpoenas*, 561 F.3d 408, 411 (5th Cir. 2009) (holding that attorney work product belongs to attorney and client). On this basis, this Court should disregard Moulton and Forensic's invocation of attorney work product.

[8] Moulton and Forensic could not be subjected to liability to LabMD for violating the work product doctrine when LabMD waived any such protection.

be produced. To the extent attorney work product may be applicable, Complaint Counsel should be permitted to assess the bases of such claims with a log required by Rule 3.38A, and to test this claim by examining Moulton.

III. MOTIONS TO QUASH AND MOTION FOR PROTECTIVE ORDER ARE NOT TIMELY

The Motions of Moulton and LabMD to quash the deposition subpoena served on Moulton are not timely. Under Rule 3.34(c), a motion to quash "shall be filed within the earlier of 10 days after service thereof or the time for compliance therewith." 16 C.F.R. § 3.34(c). Complaint Counsel effected service on Moulton's deposition subpoena on October 25, 2013, meaning that the 10-day window to file a motion to quash has long closed.

Further, LabMD has been in possession of Complaint Counsel's subpoenas since October 24, 2013. LabMD could have raised any of the arguments it is now making in its November 5, 2013 Motion for a Protective Order seeking to prevent the discovery of Moulton and Forensic but elected not to do so. *See* Respondent LabMD, Inc.'s Motion for a Protective Order, In the Matter of LabMD, Inc. Docket No. 9357 at 2, n.1 (Nov. 5, 2013). Now that this Court has ruled that the third party discovery of Moulton and Forensic should proceed, LabMD should not get another bite at the apple by raising arguments it could have previously raised.

IV. A CONTRACTUAL CONFIDENTIALITY PROVISION IS NOT A DEFENSE

Moulton and Forensic also erroneously assert that a protective order is necessary to prevent them from breaching the confidentiality provision in Forensic's contract with LabMD. This claim is without merit, as a private contractual confidentiality provision must yield to a government subpoena. *See, e.g., E.E.O.C. v. Severn Trent Svcs., Inc.*, 358 F.3d 438, 442 (7th

Cir. 2004) (private contracts cannot trump government subpoenas). Similary, private confidentiality agreements cannot serve as a bar to discovery, especially when balanced against the need for discovery in litigation. *See, e.g., Zoom Imaging, L.P. v. St. Luke's Hosp. & Health Network*, 513 F.Supp.2d 411, 417 (E.D. Pa. 2007) (holding private confidentiality agreement does not protect material from discovery).

Alternatively, the confidentiality provision in the contract between Forensic and LabMD contains an exception for publicly disclosed information (attached as Exhibit C). LabMD's public disclosure in an affidavit and book of the nature of Moulton and Forensic's work and their findings therefore vitiates any contractual requirement of Moulton and Forensic regarding disclosure of this information.

CONCLUSION

For the foregoing reasons, the Court should deny the Motions to Quash and for Protective Order regarding Scott Moulton and Forensic Strategy Services, LLC.

Dated: December 19, 2013

Respectfully submitted,

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

Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-2918 – Mehm
Facsimile: (202) 326-3062
Electronic mail: rmehm@ftc.gov

Complaint Counsel