Kelly, Andrea

From: Ramirez, Edith
Sent: Wednesday, July 23, 2014 1:53 PM
To: Ellen Doneski
Subject: RE: Rockefeller Letter to Issa Re: Improper Interference

Ellen, thank you for sending a copy of Chairman Rockefeller's letter. ~Edith

---

From: Ellen Doneski
Sent: Wednesday, July 23, 2014 1:34 PM
To: Ramirez, Edith
Subject: Rockefeller Letter to Issa Re: Improper Interference

Senator Rockefeller just sent this letter to Congressman Issa and we wanted to make sure you had a copy. Will call after mark up/hearing on cramming. Best, Ellen

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION
WASHINGTON, DC 20510-6125
WEB SITE: http://commerce.senate.gov

July 23, 2014

The Honorable Darrell E. Issa
Chairman
U.S. House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear ~~Chairman~~ Chairman Issa:

I am troubled by the impropriety of your ongoing interference with an administrative trial regarding allegations that the medical testing company LabMD, Inc. (LabMD) violated the security and privacy of almost 10,000 consumers. The trial is the result of an enforcement action brought by the Federal Trade Commission (FTC) against LabMD for lax data-security practices after discovering that consumers' sensitive personal and health information was available through a "peer-to-peer" sharing application and was being used by criminals to commit identity theft. Your interference in this legal matter is apparently going to be the subject of an upcoming hearing on July 24 in the House Committee on Oversight and Government Reform.

You purport to be concerned about allegations that a third-party company provided untruthful testimony to the FTC with regard to the LabMD breach. This allegation would be more properly raised by LabMD's defense counsel to the administrative law judge presiding over this trial. The trial process provides defense counsel with ample opportunity to impugn the veracity or integrity of a witness or evidence. It is not the job of Congress to serve as an advocate for one particular side and attempt to sway a judge who makes determinations of fact based on evidence formally presented under well-established rules and procedures.

Instead of allowing the parties in this trial to present evidence and to argue their positions before an independent fact finder, you are instead using heavy-handed, bullying tactics to undermine due process and to inappropriately assist the defendant, LabMD. As a result of your interference – including a June 11, 2014, letter to Chairwoman Edith Ramirez stating that your Committee may "immunize certain future testimony under 18 U.S.C. § 6005" – the administrative law judge presiding over this case has suspended the trial indefinitely. This delay is completely unnecessary; it needlessly forestalls resolution of this important consumer-protection case.

While Congress obviously has an important role in government oversight, I believe you have overstepped your bounds in this instance. It is not appropriate for Congress to intervene in the midst of a trial and to adversely affect its proceedings, as you have done. The inappropriate

timing and nature of your investigation are buttressed by the revelation that LabMD is being represented by a former member of your Committee staff. This raises the question of whether LabMD directly sought your help and intervention in the legal process rather than take the risk of losing on the merits at trial.

Another apparent purpose of your hearing is to express skepticism about the FTC's long-standing and well-established legal authority under Section 5 of the FTC Act to bring an action against companies like LabMD for negligent data-security practices. This skepticism is unfounded, and your public position was recently rejected by a federal judge in the FTC's data security case against Wyndham Corporation. Over the past 13 years, the Commission has initiated dozens of administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and that resulted in improper disclosures of personal information collected from consumers.

Indeed, Congress has mandated that the FTC effectively use its authority to protect consumers from "unfair or deceptive acts or practices in or affecting interstate commerce" – the very issues at the heart of the LabMD case. The legislative history of the FTC Act confirms that Congress intended to delegate broad authority "to the [C]ommission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply… There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." Against this backdrop, one must conclude that your upcoming hearing and current investigation are nothing more or less than an effort to weaken one of our nation's most important consumer-protection laws, a law that has protected generations of American consumers from scams and rip-offs.

Lastly, it is worth noting that due to Congress's repeated failure to pass strong data-security and breach notification legislation, the FTC stands as the primary federal entity protecting American consumers from harmful data breaches. Recent high-profile, large-scale data breaches -- most notably at Target – have once again raised public awareness about the need for companies to adequately secure consumer information. Because Congress remains incapable of passing meaningful data-security legislation that provides American consumers with strong protections, we must continue to rely on the FTC and its organic authority under the FTC Act to bring enforcement actions against companies that break the law. Rather than continuing to pursue your current course of interference, I would urge you to instead work to pass meaningful data-security legislation. I would welcome your assistance.

As Chairman of the Senate Committee on Commerce, Science, and Transportation, I regard the FTC as the premier consumer-protection agency in the nation. The Commission consistently seeks to carry out its mission of protecting consumers and competition, and the agency and its employees serve as an important watchdog for corporate wrongdoing. If the Commission acted improperly or otherwise relied on faulty testimony or evidence in its case against LabMD, a judge would be the proper arbiter of such an allegation at trial, not Members

of Congress. I urge you to reconsider your actions and to allow for the American legal system and the rule of law – not political theater – to resolve this case.

Sincerely,

John D. Rockefeller IV
Chairman

cc: The Honorable Elijah E. Cummings, Ranking Member

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

June 11, 2014

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

Dear Madam Chairwoman:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company upon which the Federal Trade Commission ("FTC") relied as a source of information in its enforcement action against LabMD, Inc.[1] Information the Committee recently obtained indicates that the testimony provided by company officials to federal government entities may not have been truthful.

The Committee's ongoing investigation has shown that competing claims exist about the culpability of those responsible for the dissemination of false information. It is clear at this point, however, that the information provided to the FTC is incomplete and inaccurate. A witness in the proceedings against LabMD, Inc. recently testified to the Committee that he provided incomplete or inaccurate information to the FTC regarding the origin of a "1718" document. In a transcribed interview with Committee staff, Tiversa's Chief Executive Officer, Robert Boback, testified that he received "incomplete information with regard to my testimony of FTC and LabMD."[2] He further stated that the "the original source of the disclosure was incomplete."[3] Mr. Boback testified:

> Q How did you determine that it was incomplete or that there was a problem with the spread analysis?
>
> A I had . . . [Tiversa Employee A], perform[] an analysis, again, remember, data store versus the peer to peer. So the information in the data store, [Tiversa Employee B] performed another analysis to say, what was the original source of the file from LabMD and what

[1] *See In re* LabMD, Inc., No. 9357 (Fed. Trade Comm'n Aug. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.
[2] Transcribed Interview of Robert Boback, Transcript at 129-130 (June 5, 2014) [hereinafter Boback Tr.].
[3] *Id.*

> was the disclosure, a full analysis of it which then provided to me, which expanded upon what [Tiversa Employee B] had told me when I asked [Tiversa Employee B] prior to my testimony. And the only reason why I asked [Tiversa Employee B] in the first place was because [Tiversa Employee B] was the analyst on it at the time when it was found, so I asked the analyst who was most familiar with this. I didn't know [Tiversa Employee B] was going to provide me with less than accurate information.
>
> * * *
>
> Q So at the time that you were first made aware of the 1718 document in April, May of 2008, Tiversa employees had not conducted the spread analysis?
>
> A No.
>
> Q And you did not know the original source of the 1718 document?
>
> A I did not. No.
>
> * * *
>
> Q Did there come a point at which a Tiversa employee determined who the original source of the 1718 document was?
>
> A Well, that's – yes. A Tiversa employee told me who the original source was . . . just before I testified . . . in the deposition [in the FTC LabMD case] in November of last year. And, subsequently, we have done a new search and found that the origin was different than what was provided to me . . . in November.

The Committee brings this matter to your attention because this information bears directly on the ongoing proceeding against LabMD, Inc. The Committee is currently considering next steps with regard to its own investigation, including the possibility of holding hearings, agreeing to hear certain testimony in executive session, and, based on information provided, to immunize certain future testimony pursuant to 18 U.S.C. § 6005. The Committee may request documents and access to relevant FTC witnesses. It is my expectation that you and your staff will cooperate fully with any subsequent requests for documents or transcribed witness interviews.

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

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

William A. Sherman II, Counsel, LabMD, Inc.

Laura Riposo VanDruff, Complain Counsel, U.S. Federal Trade Commission

William A. Burck, Quinn Emanuel Urquhart & Sullivan LLP

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Thursday, July 17, 2014 2:24 PM
To: 'Ash, Michelle'; Berroya, Meghan
Subject: RE: hearing

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks Michelle,

Hi Meghan, I would love to talk to you at your earliest convenience. My number is (202) 326-2946.

Jeanne

Jeanne Bumpus
Director
Office of Congressional Relations
Federal Trade Commission
326-2946

From: Ash, Michelle [mailto:Michelle.Ash@mail.house.gov]
Sent: Thursday, July 17, 2014 2:21 PM
To: Berroya, Meghan; Bumpus, Jeanne
Subject: hearing

Meghan is with Oversight and Government Reform, Jeanne Bumpus is with FTC congressional. Meet each other. Cheers.

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Monday, July 21, 2014 12:48 PM
To: 'Nagle, Paul'
Subject: RE: Hearing in OGR re: Section 5

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks Paul.

From: Nagle, Paul [mailto:Paul.Nagle@mail.house.gov]
Sent: Monday, July 21, 2014 12:48 PM
To: Bumpus, Jeanne
Subject: RE: Hearing in OGR re: Section 5

Thanks for the heads up – that had caught my eye as well. We will monitor the hearing from afar for now.

From: Bumpus, Jeanne [mailto:JBumpus@ftc.gov]
Sent: Monday, July 21, 2014 12:19 PM
To: Nagle, Paul
Subject: Hearing in OGR re: Section 5

Paul,

I wanted to make you are aware that the Oversight and Government Reform Committee has noticed a hearing for this Thursday morning entitled "The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury." We expect they will discuss data security and the LabMD case. We hope to learn more about the hearing this afternoon.

Jeanne

Kelly, Andrea

From: Bumpus, Jeanne
Sent: Wednesday, July 23, 2014 2:16 PM
To: Christian Fjeld; Vandecar, Kim
Subject: RE: Letter

Follow Up Flag: Follow up
Flag Status: Flagged

Thanks for sharing it.

From: Christian Fjeld
Sent: Wednesday, July 23, 2014 1:42 PM
To: Bumpus, Jeanne; Vandecar, Kim
Subject: Letter

Jeanne and Kim – attached is a letter that Chairman Rockefeller sent to Chairman Issa with regard to his ongoing investigation and upcoming hearing on LabMD. Call me with any questions.

Christian

Christian Tamotsu Fjeld
Senior Counsel
Senate Committee on Commerce, Science and Transportation
428 Hart Office Building
Washington, DC 20510
p: (202) 224-1270 f: (202) 228-0327

Kelly, Andrea

From: Benway, Kathleen (Commerce) <Kathleen_Benway@commerce.senate.gov>
Sent: Monday, July 21, 2014 9:36 AM
To: Vandecar, Kim; Bumpus, Jeanne; Simons, Claudia A.
Subject: RE: The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury | Committee on Oversight & Government Reform

Follow Up Flag: Follow up
Flag Status: Flagged

I figured

From: Vandecar, Kim [mailto:KVANDECAR@ftc.gov]
Sent: Monday, July 21, 2014 9:34 AM
To: Benway, Kathleen (Commerce); Bumpus, Jeanne; Simons, Claudia A.
Subject: RE: The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury | Committee on Oversight & Government Reform

Thanks. We saw it yesterday.

From: Benway, Kathleen (Commerce) [mailto:Kathleen_Benway@commerce.senate.gov]
Sent: Monday, July 21, 2014 9:33 AM
To: Bumpus, Jeanne; Vandecar, Kim; Simons, Claudia A.
Subject: FW: The Federal Trade commission and Its Section 5 Authority: Prosecutor, Judge, and Jury | Committee on Oversight & Government Reform

Link to the Issa hearing is up. No witnesses listed.

http://oversight.house.gov/hearing/federal-trade-commission-section-5-authority-prosecutor-judge-jury-2/

Kelly, Andrea

From: Vandecar, Kim
Sent: Wednesday, June 18, 2014 3:22 PM
To: 'Taylor, Shannon'
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Follow Up Flag: Follow up
Flag Status: Flagged

I'll be in touch shortly.

From: Taylor, Shannon [mailto:shannon.taylor@mail.house.gov]
Sent: Wednesday, June 18, 2014 3:12 PM
To: Vandecar, Kim
Subject: Fw: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

We definitely need to talk now. Let me know if Friday late morning would work. If not we'll find another time.

From: Marrero, Alexa
Sent: Wednesday, June 18, 2014 03:09 PM
To: Nagle, Paul; Taylor, Shannon
Subject: FW: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

ICYMI

From: Watkins, Becca
Sent: Wednesday, June 18, 2014 3:01 PM
Subject: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

June 18th, 2014
Contact: Becca Watkins, 202.225.0037

Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

WASHINGTON –House Oversight and Government Reform Committee Chairman Darrell Issa, R-Calif., sent a letter to Federal Trade Commission's (FTC) Acting Inspector General Kelly Tshibaka last night requesting that the IG's office

investigate the FTC's relationship with Tiversa, Inc. The Committee has substantial concerns about the reliability of the information Tiversa provided to the FTC and the relationship between the FTC and Tiversa.

In 2008, Tiversa allegedly discovered a document pertaining to LabMD, Inc. containing the personal information of thousands of patients on a peer-to-peer network. Tiversa contacted LabMD in May 2008, explaining that it believed it had identified a data breach at the company and offering "remediation" services through a professional services agreement. LabMD did not accept Tiversa's offer because LabMD believed it had contained and resolved the data breach. Tiversa, through an entity known as the Privacy Institute, later provided the FTC with a document it created that included information about LabMD, among other companies. Tiversa allegedly provided information to the FTC about companies that refused to buy its services. In the case of LabMD, after Tiversa provided information to the FTC, the Commission sought an enforcement action against the company under its Section 5 authority related to deceptive and unfair trade practices. New information has surfaced indicating that information Tiversa supplied to the FTC may have been inaccurate

"The possibility that inaccurate information played a role in the FTC's decision to initiate enforcement actions against LabMD is a serious matter," said Chairman Issa in today's letter. "The FTC's enforcement actions have resulted in serious financial difficulties for the company. Additionally, the alleged collaboration between the FTC and Tiversa, a company which has now admitted that the information it provided to federal government entities—including the FTC—may be inaccurate, creates the appearance that the FTC aided a company whose business practices allegedly involve disseminating false data about the nature of data security breaches."

The letter continues: "Further, the Committee has received information from current and former Tiversa employees indicating a lack of truthfulness in testimony Tiversa provided to federal government entities. The Committee's investigation is ongoing, and competing claims exist about the culpability of those responsible for the dissemination of false information. It is now clear, however, that Tiversa provided incomplete and inaccurate information to the FTC. "

Read the letter and embedded below.

June 16, 2014

Ms. Kelly Tshibaka
Acting Inspector General
Federal Trade Commission
Room CC-5206
600 Pennsylvania Avenue NW
Washington, D.C. 20580

Dear Ms. Tshibaka:

The Committee on Oversight and Government Reform is investigating the activities of Tiversa, Inc., a company that provided information to Federal Trade Commission in an enforcement action against LabMD, Inc.[1] In 2008, Tiversa allegedly discovered a document containing the personal information of thousands of patients on a peer-to-peer network.[2] Tiversa contacted LabMD in May 2008, explaining that it believed it had identified a data breach at the company and offering "remediation" services through a professional services agreement.[3] LabMD did not accept Tiversa's offer because LabMD believed it had contained and resolved the data breach. Tiversa, through an entity

known as the Privacy Institute, later provided the FTC with a document it created that included information about LabMD, among other companies.[4] Apparently, Tiversa provided information to the FTC about companies that refused to buy its services. In the case of LabMD, after Tiversa provided questionable information to the FTC, the Commission sought an enforcement action against the company under its Section 5 authority related to deceptive and unfair trade practices.[5]

In addition to concerns about the merits of the enforcement action with respect to the FTC's jurisdiction, the Committee has substantial concerns about the reliability of the information Tiversa provided to the FTC, the manner in which Tiversa provided the information, and the relationship between the FTC and Tiversa. For instance, according to testimony by Tiversa CEO Robert Boback, the Committee has learned of allegations that Tiversa created the Privacy Institute in conjunction with the FTC specifically so that Tiversa could provide information regarding data breaches to the FTC in response to a civil investigative demand. The Committee has also learned that Tiversa, or the Privacy Institute, may have manipulated information to advance the FTC's investigation. If these allegations are true, such coordination between Tiversa and the FTC would call into account the LabMD enforcement action, and other FTC regulatory matters that relied on Tiversa supplied information.

Further, the Committee has received information from current and former Tiversa employees indicating a lack of truthfulness in testimony Tiversa provided to federal government entities. The Committee's investigation is ongoing, and competing claims exist about the culpability of those responsible for the dissemination of false information. It is now clear, however, that Tiversa provided incomplete and inaccurate information to the FTC. In a transcribed interview with Oversight and Government Reform Committee staff, Boback testified that he received "incomplete information with regard to my testimony of FTC and LabMD."[6] He stated that he now knows "[t]he original source of the disclosure was incomplete."[7] Mr. Boback testified:

> Q How did you determine that it was incomplete or that there was a problem with the spread analysis?
>
> A I had . . . [Tiversa Employee A] perform[] an analysis, again, remember, data store versus the peer to peer. So the information in the data store, he performed another analysis to say, what was the original source of the file from LabMD and what was the disclosure, a full analysis of it which then provided to me, which expanded upon what [Tiversa Employee B] had told me when I asked [Tiversa Employee B]prior to my testimony. And the only reason why I asked [Tiversa Employee B] in the first place was because [Tiversa Employee B] was the analyst on it at the time when it was found, so I asked the analyst who was most familiar with this. I didn't know [Tiversa Employee B] was going to provide me with less than accurate information.[8]
>
> * * *
>
> Q So at the time that you were first made aware of the 1718 document in April, May of 2008, Tiversa employees had not conducted the spread analysis?
>
> A No.
>
> Q And you did not know the original source of the 1718 document?
>
> A I did not. No.
>
> * * *
>
> Q Did there come a point at which a Tiversa employee determined who the original source of the 1718 document was?

A Well, that's – yes. A Tiversa employee told me who the original source was … just before I testified … in the deposition [in the FTC LabMD case] in November of last year. And, subsequently, we have done a new search and found that the origin was different than what was provided to me . . . in November.[9]

The possibility that inaccurate information played a role in the FTC's decision to initiate enforcement actions against LabMD is a serious matter. The FTC's enforcement actions have resulted in serious financial difficulties for the company.[10] Additionally, the alleged collaboration between the FTC and Tiversa, a company which has now admitted that the information it provided to federal government entities—including the FTC—may be inaccurate, creates the appearance that the FTC aided a company whose business practices allegedly involve disseminating false data about the nature of data security breaches. The Committee seeks to understand the motivations underlying the relationship between Tiversa and the FTC.

The Committee is currently considering next steps, including the possibility of holding hearings, agreeing to take certain testimony in executive session, and, based on information provided, to immunize certain future testimony pursuant to 18 U.S.C. § 6005. Concurrent with the Committee's investigative efforts, I request that you undertake a full review of the FTC's relationship with Tiversa.

Specifically, I ask that your office examine the following issues:

1. FTC procedures for receiving information that it uses to bring enforcement actions pursuant to its authority under Section 5, and whether FTC employees have improperly influenced how the agency receives information.

2. The role played by FTC employees, including, but not limited to, Alain Sheer and Ruth Yodaiken, in the Commission's receipt of information from Tiversa, Inc. through the Privacy Institute or any other entity, and whether the Privacy Institute or Tiversa received any benefit for this arrangement.

3. The reasons for the FTC's issuance of a civil investigative demand to the Privacy Institute instead of Tiversa, the custodian of the information.

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 about this request, please contact Tyler Grimm or Jennifer Barblan of the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,

_____

Darrell Issa
Chairman

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

Becca Glover Watkins
Communications Director

House Committee on Oversight and Government Reform
Chairman Darrell Issa
Rayburn 2157
202.731.7234 - Blackberry
202.225.0037 - Press
202.225.5074 - Committee Main
becca.watkins@mail.house.gov
http:// oversight.house.gov/

[1] *See* Complaint, *In re* LabMD, Inc., No. 9357 (Fed. Trade Comm'n, Aug. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.
[2] Respondent LabMD, Inc.'s Answer and Defenses to Administrative Complaint, *In re* LabMD, Inc., No. 9357 (Fed. Trade Comm'n, Sept. 17, 2013), at 5.
[3] Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, *In re* LabMD, Inc., No. 9357 (Fed. Trade Comm'n, Nov. 12, 2013), at 5.
[4] 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.].
[5] *See generally* 15 U.S.C. § 45.
[6] Boback Tr. at 129.
[7] *Id*.
[8] *Id*. at 129-130.
[9] *Id*. at 162-163.
[10] Rachel Louise Ensign, *FTC Cyber Case Has Nearly Put Us Out of Business, Firm Says*, WALL ST. J., Jan. 28, 2014, http://blogs.wsj.com/riskandcompliance/2014/01/28/ftc-cyber-case-has-nearly-put-us-out-of-business-firm-says/.

Kelly, Andrea

From: Vandecar, Kim
Sent: Wednesday, June 18, 2014 5:27 PM
To: 'Taylor, Shannon'
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Follow Up Flag: Follow up
Flag Status: Flagged

Yes.

From: Taylor, Shannon [mailto:shannon.taylor@mail.house.gov]
Sent: Wednesday, June 18, 2014 5:25 PM
To: Vandecar, Kim
Subject: Re: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

11am on Friday in H2-255?

From: Vandecar, Kim [mailto:KVANDECAR@ftc.gov]
Sent: Wednesday, June 18, 2014 04:10 PM
To: Taylor, Shannon
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

It will. Tell us when and where. Daniel Kaufman, Deputy Director of BCP will come along with one of our General Counsels, Maneesha, Jeanne and myself.

Duplicate

Kelly, Andrea

From: Taylor, Shannon <shannon.taylor@mail.house.gov>
Sent: Wednesday, June 18, 2014 5:29 PM
To: Vandecar, Kim
Subject: Re: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

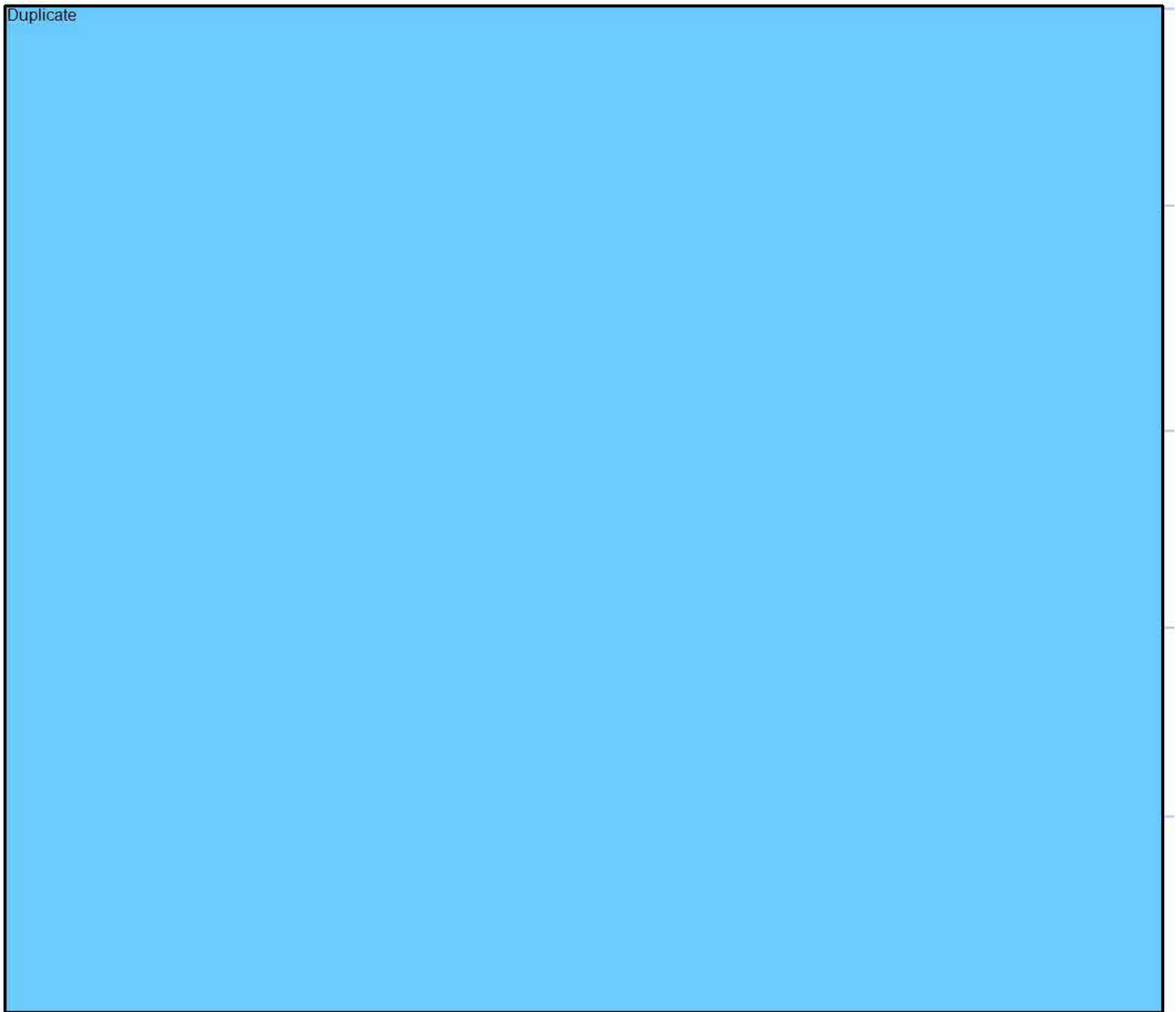
Follow Up Flag: Follow up
Flag Status: Flagged

Second floor of ford btwn the elevator banks.

From: Vandecar, Kim [mailto:KVANDECAR@ftc.gov]
Sent: Wednesday, June 18, 2014 05:28 PM
To: Taylor, Shannon
Subject: RE: RELEASE: Issa to FTC Watchdog: Investigate Allegations of Corporate Blackmail

Where is that?

Duplicate



Kelly, Andrea

From: Vandecar, Kim
Sent: Friday, July 11, 2014 6:23 PM
To: 'Shannon.Weinberg@mail.house.gov'; 'paul.nagle@mail.house.gov'
Cc: 'Kirby.Howard@mail.house.gov'; Oxford, Clinton P.
Subject: Fw: QFRs for Data Security Hearing House Subcommittee on Commerce.docx
Attachments: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Follow Up Flag: Follow up
Flag Status: Flagged

Final FTC QFR's on data security

From: Vandecar, Kim
Sent: Friday, July 11, 2014 02:28 PM
To: Howard, Kirby (Kirby.Howard@mail.house.gov) <Kirby.Howard@mail.house.gov>
Subject: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Kirby,

Can you use this version instead please?

Thanks,

Kim

Additional Questions for the Record
Subcommittee on Commerce, Manufacturing, and Trade
"Protecting Consumer Information: Can Breaches Be Prevented?"
February 5, 2014

The Honorable Lee Terry

1. You testified that legislation would "strengthen [FTC's] existing authority governing data security standards." If you already have the authority to pursue data security enforcement actions now, why do you need a new law? What would change with such a law?

   The Commission has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases.

   The Commission supports federal legislation that would (1) strengthen its existing tools to address companies' inadequate practices for securing consumers' data and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Such legislation is important for a number of reasons. First, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Second, enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology when implementing the legislation.

2. You testified that "although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring…consumers are protected." Does that mean you believe preemption is appropriate in this area?

   The Commission has expressed support for a federal data security and breach notification law that would preempt state law, but only if such a standard is sufficiently strong and the states are given the ability to enforce the law. If a consistent nationwide standard came at the expense of weakening existing state legal protections for consumers' information, the Commission would not support the law.

3. You testify the Commission supports a Federal law that requires companies "in appropriate circumstances," to provide notification to consumers. Can you describe what "appropriate" circumstances are? Are there occasions where notification could cause unnecessary problems for consumers and should not occur (e.g., cancelling a credit card when no account information was compromised)?

   It is important for both consumers and businesses that the trigger for breach notification is balanced. We want to ensure that consumers learn about breaches that could result in identity theft, fraud, or other harm so they can take steps to protect themselves, but we do not want to notify consumers when the risk of harm is negligible,

as over-notification could cause consumers to become confused or to become numb to the notices they receive.

The following standard strikes the right balance: When an entity discovers a breach of security, the entity should be required to notify every consumer whose personal information was, or there is a reasonable basis to conclude was, accessed by an unauthorized person, unless the entity can demonstrate that there is no reasonable risk of identity theft, fraud, or other harm. (Of course, breach notification would only be triggered if specified categories of personal information have been the subject of a breach.) This standard balances the need for consumers to know when their information has been breached against the threat of over-notification for breaches that have no reasonable risk of harm.

4. You testify the Commission has settled 50 cases against businesses that it charged with failure to provide reasonable and appropriate protections for consumers' personal information. That does not include non-profits because the FTC's jurisdiction does not extend to those entities. With regard to data security, should the Commission have authority over non-profits? We have heard of universities and colleges suffering data breaches. Are they a common source of data breaches?

   Yes, the Commission believes it should have jurisdiction over non-profits in this area. A substantial number of reported breaches have involved non-profit universities and health systems. Enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

5. Has the Commission pursued any data security cases that resulted in litigation instead of a settlement?

   Most companies have chosen to settle the Commission's data security claims. However, the Commission currently has two data security cases in active litigation. *FTC v. Wyndham Worldwide Corp.* is pending in the federal district court in the District of New Jersey.[1] The Commission also approved the filing of a case in the FTC's administrative court, *In the Matter of LabMD*.[2]

6. How does the FTC enforce its "unfairness" standard? What principles guide the FTC so that businesses know when they might run afoul of the unfairness standard?

   A company's practices are unfair if they cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[3] In the Commission's data security cases, reasonableness is the lynchpin. In determining whether a company's

---

[1] *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J.).
[2] *LabMD, Inc.*, No. C-9357 (F.T.C. compl. filed Aug. 28, 2013), *available at* http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf.
[3] *See* 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

data security practices are reasonable the Commission considers: the sensitivity and volume of consumer information a business holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The reasonableness test is designed to be flexible; reasonable data security safeguards should be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

In addition to the more than 50 data security consent orders, which provide guidance to businesses about what constitutes reasonable security, the Commission also has published business guidance and educational materials about good data security practices for companies. We have emphasized a process-based approach that includes: designating a person to be responsible for data security; conducting risk assessments; designing a program to address the risks identified, including training, security and incident response; and monitoring the program and updating it as necessary.

7. Has the FTC ever suffered a data breach?

We are not aware of any successful intrusions or infiltrations into the FTC network. Like other federal agencies and companies in the private sector, we are constantly under attack, and we use defense-in-depth (meaning multiple layers of security controls, such as firewalls, anti-virus and anti-spam tools, internet filters), continuous monitoring, and other methods to protect our information systems and the data they contain.

8. You mentioned that more than 16 million Americans have been victims of identity theft. What counts as identity theft for this purpose? Does it include cases where someone else uses your credit card number even if you end up without any financial loss?

The figure cited in the Commission's written testimony is from the Bureau of Justice Statistics report, "Victims of Identity Theft, 2012," which is the most recent BJS study of identity theft victims.[4] For the purposes of that report, identity theft victims are defined as persons age 16 or older who experienced one or more of the following incidents in 2012: unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account); unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account); or misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information). According to the report, direct and indirect identity theft losses amounted to approximately $24.7 billion in 2012.

Fraud detection programs are not perfect, so consumers are not reimbursed for all fraudulent charges placed on their accounts. Even when victims are ultimately reimbursed for out-of-pocket financial losses from a breach, this does not mean that they did not experience other, non-compensated harms from the breach. Consumers affected by breaches should constantly monitor their financial accounts for unauthorized charges. If consumers discover such charges, they must notify their credit and debit card issuers, close accounts, cancel cards, and wait for new cards to arrive. For those consumers with automatic bill pay, they must alert companies about the new account numbers to prevent late fees and other charges. Victims of identity theft can spend months reporting instances of fraud to creditors and reporting bureaus to restore their credit. Victims are not compensated for the economic cost from these expenditures of time.

The Honorable Jan Schakowsky

1. On January 10, 2014, Target announced that certain customer information – separate from the payment card data already revealed to have been stolen – had also been taken during the breach of its network systems in November and December 2013. This information included names, mailing addresses, phone numbers or email addresses for up to 70 million individuals.

    a. What are the top risks to consumers whose names and contact information are stolen, including those Target customers who are among the 70 million? Please list them.

Personal information that is non-financial still requires protection, because it can be used to perpetuate fraud and identity theft. For instance, bad actors can use email addresses to perpetrate phishing attacks, send spam, or target users for malware, the latter of which can be used to install keyloggers or other technology to capture even more personal information. Moreover, targeted fraud becomes increasingly effective

[4] Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

the more personal information a criminal has about a consumer. For example, many consumers still use their email address as a user name on accounts. That, along with access to other personal information, may increase the danger of a criminal being able to ascertain a password and access a financial or other account or to perpetrate identity theft.

b. Members and witnesses at recent congressional hearings on commercial data breaches have discussed at length potential enhancements to payment card security technology, such as the implementation of chip-and-PIN systems. At the Subcommittee hearing on February 5, 2014 – while stressing that the Commission does not recommend any particular technology – you indicated that "we would support any steps that are taken at the payment card system end to protect or better protect consumer information." I believe it is important for retailers, issuers, and the payment card industry to urgently work together to improve card security. However, even if all the stakeholders involved agree to make payment card data as secure as possible, am I correct to understand that it is your position that that Congress should still separately address the overall security of personal data, including non-financial data, collected or stored by commercial entities?

That is correct. The Commission is aware of this developing technology, and according to some reports, it should be a positive step toward strengthening payment card security. However, this technology does not protect other information, such as health information, location information, or SSNs.

All companies that collect and handle consumer information should be required to implement reasonable data security measures. Reasonableness is the appropriate standard because it allows a company flexibility to develop a data security program based on factors such as the sensitivity and volume of consumer information it holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

The Commission reiterates our call for data security and breach notification legislation that would: (1) give us the authority to obtain civil penalties, an important remedy for deterring violations; (2) enable the FTC to bring cases against non-profits, such as hospitals and educational institutions, where many breaches occur; and (3) providing rulemaking authority under the Administrative Procedure Act, enabling the FTC to respond to changes in technology when implementing the legislation.

I believe the breach of marketing data can be a serious threat to consumers. As I said in response to questioning at the Subcommittee's hearing, names and contact information can be used in phishing and social engineering schemes to try to perpetrate identity theft – and while harm from payment card breaches tends to be acute, harm from non-financial breaches tends to linger. In short, identity theft lasts; with chronic effects on consumers that can cost them everything they own.

c. Do you agree that a breach of names and contact information can have a serious long-term impact on consumers, if used to trick them to give up sensitive identity data? Please explain your answer.

Yes. As discussed above, such information can be used to perpetrate fraud and identity theft, which can have lasting impacts on consumers' credit scores, in addition to the economic value of time lost and possible financial loss.

2. On January 31, 2014, the FTC announced the 50th data security settlement in its program of enforcement against those who fail to reasonably protect consumers' personal information. These settlements have been used to protect millions of consumers from unfair or deceptive practices that leave at risk sensitive information like usernames and passwords, Social Security numbers, and health, financial, and children's data. I commend your dedication to this issue.

   Yet, during questioning at the Senate Banking Committee hearing on this topic on February 3, 2014, a Senator pointed out that with so many data breaches each year, 50 cases since 2002 may be commendable, but it may not be enough.

   a. Of course, all breaches do not rise to the level of FTC action, but can you please illustrate how the FTC uses its current legal framework to help with general deterrence, and how authorization to the FTC of new authorities, such as rulemaking authority under the Administrative Procedure Act and broader civil penalty authority, would increase the FTC's ability to deter unfair or deceptive data security practices?

Since 2002, the FTC has brought a steady stream of data security cases – resulting in more than 50 consent orders, and we have also issued extensive consumer and business education materials. During much of this time, we have been the only federal agency sending the message to a wide range of businesses, both small and large, across many sectors, of the need to maintain reasonable security to protect consumer data. Our complaints provide examples of data security practices that did not meet our flexible reasonableness test, and our consent orders serve as templates for best practices for companies setting up and implementing successful information security programs. In addition, we issue extensive guidance for consumers and businesses – especially small businesses – about how to safeguard consumer data. I believe that collectively the FTC's work in this area has helped promote appropriate investment in infrastructure and personnel to address the security of consumer data.

But, plainly, more needs to be done, and a unanimous Commission has concluded that the time has come for Congress to enact strong federal data security and breach notification legislation. We currently lack authority under Section 5 to obtain civil penalties, which are critical to appropriate deterrence of lax security practices. Likewise, enabling the FTC to bring cases against non-profits, over which we presently lack authority, would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, APA rulemaking would give us flexibility in implementing the statute by

making changes where appropriate – for example, to the definitions – to respond to changes in technology and changing threats.

b. Recent newspaper commentary has suggested that by seeking to strengthen its data security authority, the FTC is acknowledging that it currently lacks the authority to police companies' data security practices. How do you respond to such an assertion?

The Commission principally has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases to date. In fact, a federal district court recently affirmed the FTC's authority to use Section 5 in the data security area.[5]

The Commission has called for data security legislation that would strengthen its existing tools and authority to help us in this endeavor, namely, civil penalty authority, jurisdiction over non-profits, a nationwide breach notice requirement to be enforced by the FTC and the states, and APA rulemaking to ensure we have adequate flexibility to respond to new technology and threats in implementing the statute.

The Honorable Jerry McNerney

1. Thank you for your leadership within the FTC, especially with regards to the work that is being done on privacy issues. What sort of authority does the Commission have or need from Congress to institute nationwide breach notification processes?

The FTC has authority to investigate breaches and bring civil enforcement actions under Section 5 of the FTC Act for deceptive or unfair acts or practices – such as deceptively claiming to reasonably safeguard consumer data. We have authority to seek equitable remedies for violations of Section 5, which does not include civil penalties.[6] The FTC also generally lacks authority to require companies to issue notification to affected consumers to alert them to a breach of their personal information (with the exception of our narrow scope of authority under the HI-TECH Act). We similarly lack authority over non-profits, which have been the source of a number of breaches. To remedy these gaps, a unanimous Commission has called on Congress to enact legislation to pass a nationwide breach notification law to apply to all companies under the FTC's jurisdiction – expanding that jurisdiction to include non-profits –and to give the Commission civil penalty authority and authority to flexibly respond to changes in technology in implementing the law via APA rulemaking.

2. Businesses are understandably leery of the idea of additional regulations, but many people that I have talked with agree that a national standard is easier to deal with than varying state standards when it comes to data breach notification rules. In your opinion, how can the FTC

[5] *See F.T.C. v. Wyndham Worldwide Corp*, No. 2:13-cv-01887-ES-JAD, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *petition for leave to appeal filed* (3d Cir. July 3, 2014).

[6] By contrast, the FTC has civil penalty authority under the Fair Credit Reporting Act for security violations by "consumer reporting agencies," such as the national credit bureaus.

and Congress best work together to come up with a national standard that doesn't impose unfairly upon states' rights?

Breach notification and data security standards at the federal level, with appropriate preemption of state law as discussed below, would extend notifications to all citizens nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A federal law would create uniform protections for all American consumers. However, our support for a federal law that would preempt state law has been conditioned on both a standard that is sufficiently strong and on giving states the ability to enforce the law, an important role for state Attorneys General.

The Honorable Peter Welch

1. We've seen the FTC take a strong leadership position on many issues, not only bringing enforcement actions but also convening experts from industry and academia at workshops. These workshops have been valuable opportunities for the FTC to write reports on what it learns, including guidance to companies when appropriate. It seems to me like an annual workshop and report on data security would be valuable given the recent problems companies have been having -- can we expect the FTC to have such a workshop soon?

   Thank you for your recognition of the FTC's leadership on many issues and the value of our use of enforcement actions and public workshops. As you may know, emerging areas in privacy and security are frequent subjects of FTC workshops, studies, and reports. For instance, in June of last year, we held a workshop on threats to mobile security, in which we convened a group of leading experts to discuss mobile malware, the role of platforms in security, and ways to improve security in the mobile ecosystem.[7] Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy and security implications of a number of new technologies in the marketplace, including mobile device tracking, alternative scoring products, and apps and devices that collect consumer-generated health data.[8] At the Commission's November 2013 conference on the Internet of Things, much of the discussion focused on security challenges presented by "smart" devices.[9]

   Moreover, the FTC just published its first annual "Privacy and Data Security Update," which is an overview of the FTC's enforcement, policy initiatives, and consumer

---

[7] *See* Mobile Security: Potential Threats and Solutions (June 4, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions.

[8] *See* FTC to Host Spring Seminars on Emerging Consumer Privacy Issues, *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

[9] *See* Internet of Things - Privacy and Security in a Connected World (Nov. 19, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

outreach and business guidance in the areas of privacy and data security from January 2013-March 2014.[10] We expect to update this document every year.

[10] Federal Trade Commission Staff, 2014 Privacy and Security Update (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

Kelly, Andrea

From: Vandecar, Kim
Sent: Thursday, July 17, 2014 2:27 PM
To: 'will.wallace@mail.house.gov'; 'Michelle.Ash@mail.house.gov'
Subject: Fw: QFRs for Data Security Hearing House Subcommittee on Commerce.docx
Attachments: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Follow Up Flag: Follow up
Flag Status: Flagged

From: Vandecar, Kim
Sent: Wednesday, July 16, 2014 12:52 PM
To: Eichorn, Mark
Subject: FW: QFRs for Data Security Hearing House Subcommittee on Commerce.docx

Additional Questions for the Record
Subcommittee on Commerce, Manufacturing, and Trade
"Protecting Consumer Information: Can Breaches Be Prevented?"
February 5, 2014

The Honorable Lee Terry

1. You testified that legislation would "strengthen [FTC's] existing authority governing data security standards." If you already have the authority to pursue data security enforcement actions now, why do you need a new law? What would change with such a law?

   The Commission has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases.

   The Commission supports federal legislation that would (1) strengthen its existing tools to address companies' inadequate practices for securing consumers' data and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Such legislation is important for a number of reasons. First, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Second, enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC to respond to changes in technology when implementing the legislation.

2. You testified that "although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring…consumers are protected." Does that mean you believe preemption is appropriate in this area?

   The Commission has expressed support for a federal data security and breach notification law that would preempt state law, but only if such a standard is sufficiently strong and the states are given the ability to enforce the law. If a consistent nationwide standard came at the expense of weakening existing state legal protections for consumers' information, the Commission would not support the law.

3. You testify the Commission supports a Federal law that requires companies "in appropriate circumstances," to provide notification to consumers. Can you describe what "appropriate" circumstances are? Are there occasions where notification could cause unnecessary problems for consumers and should not occur (e.g., cancelling a credit card when no account information was compromised)?

   It is important for both consumers and businesses that the trigger for breach notification is balanced. We want to ensure that consumers learn about breaches that could result in identity theft, fraud, or other harm so they can take steps to protect themselves, but we do not want to notify consumers when the risk of harm is negligible,

as over-notification could cause consumers to become confused or to become numb to the notices they receive.

The following standard strikes the right balance: When an entity discovers a breach of security, the entity should be required to notify every consumer whose personal information was, or there is a reasonable basis to conclude was, accessed by an unauthorized person, unless the entity can demonstrate that there is no reasonable risk of identity theft, fraud, or other harm. (Of course, breach notification would only be triggered if specified categories of personal information have been the subject of a breach.) This standard balances the need for consumers to know when their information has been breached against the threat of over-notification for breaches that have no reasonable risk of harm.

4. You testify the Commission has settled 50 cases against businesses that it charged with failure to provide reasonable and appropriate protections for consumers' personal information. That does not include non-profits because the FTC's jurisdiction does not extend to those entities. With regard to data security, should the Commission have authority over non-profits? We have heard of universities and colleges suffering data breaches. Are they a common source of data breaches?

   Yes, the Commission believes it should have jurisdiction over non-profits in this area. A substantial number of reported breaches have involved non-profit universities and health systems. Enabling the FTC to bring cases against non-profits would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

5. Has the Commission pursued any data security cases that resulted in litigation instead of a settlement?

   Most companies have chosen to settle the Commission's data security claims. However, the Commission currently has two data security cases in active litigation. *FTC v. Wyndham Worldwide Corp.* is pending in the federal district court in the District of New Jersey.[1] The Commission also approved the filing of a case in the FTC's administrative court, *In the Matter of LabMD*.[2]

6. How does the FTC enforce its "unfairness" standard? What principles guide the FTC so that businesses know when they might run afoul of the unfairness standard?

   A company's practices are unfair if they cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.[3] In the Commission's data security cases, reasonableness is the lynchpin. In determining whether a company's

---

[1] *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J.).
[2] *LabMD, Inc.*, No. C-9357 (F.T.C. compl. filed Aug. 28, 2013), *available at* http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf.
[3] *See* 15 U.S.C. § 45(n); Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

data security practices are reasonable the Commission considers: the sensitivity and volume of consumer information a business holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The reasonableness test is designed to be flexible; reasonable data security safeguards should be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

In addition to the more than 50 data security consent orders, which provide guidance to businesses about what constitutes reasonable security, the Commission also has published business guidance and educational materials about good data security practices for companies. We have emphasized a process-based approach that includes: designating a person to be responsible for data security; conducting risk assessments; designing a program to address the risks identified, including training, security and incident response; and monitoring the program and updating it as necessary.

7. Has the FTC ever suffered a data breach?

We are not aware of any successful intrusions or infiltrations into the FTC network. Like other federal agencies and companies in the private sector, we are constantly under attack, and we use defense-in-depth (meaning multiple layers of security controls, such as firewalls, anti-virus and anti-spam tools, internet filters), continuous monitoring, and other methods to protect our information systems and the data they contain.

8. You mentioned that more than 16 million Americans have been victims of identity theft. What counts as identity theft for this purpose? Does it include cases where someone else uses your credit card number even if you end up without any financial loss?

The figure cited in the Commission's written testimony is from the Bureau of Justice Statistics report, "Victims of Identity Theft, 2012," which is the most recent BJS study of identity theft victims.[4] For the purposes of that report, identity theft victims are defined as persons age 16 or older who experienced one or more of the following incidents in 2012: unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account); unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account); or misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information). According to the report, direct and indirect identity theft losses amounted to approximately $24.7 billion in 2012.

Fraud detection programs are not perfect, so consumers are not reimbursed for all fraudulent charges placed on their accounts. Even when victims are ultimately reimbursed for out-of-pocket financial losses from a breach, this does not mean that they did not experience other, non-compensated harms from the breach. Consumers affected by breaches should constantly monitor their financial accounts for unauthorized charges. If consumers discover such charges, they must notify their credit and debit card issuers, close accounts, cancel cards, and wait for new cards to arrive. For those consumers with automatic bill pay, they must alert companies about the new account numbers to prevent late fees and other charges. Victims of identity theft can spend months reporting instances of fraud to creditors and reporting bureaus to restore their credit. Victims are not compensated for the economic cost from these expenditures of time.

The Honorable Jan Schakowsky

1. On January 10, 2014, Target announced that certain customer information – separate from the payment card data already revealed to have been stolen – had also been taken during the breach of its network systems in November and December 2013. This information included names, mailing addresses, phone numbers or email addresses for up to 70 million individuals.

    a. What are the top risks to consumers whose names and contact information are stolen, including those Target customers who are among the 70 million? Please list them.

Personal information that is non-financial still requires protection, because it can be used to perpetuate fraud and identity theft. For instance, bad actors can use email addresses to perpetrate phishing attacks, send spam, or target users for malware, the latter of which can be used to install keyloggers or other technology to capture even more personal information. Moreover, targeted fraud becomes increasingly effective

[4] Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

the more personal information a criminal has about a consumer. For example, many consumers still use their email address as a user name on accounts. That, along with access to other personal information, may increase the danger of a criminal being able to ascertain a password and access a financial or other account or to perpetrate identity theft.

b. Members and witnesses at recent congressional hearings on commercial data breaches have discussed at length potential enhancements to payment card security technology, such as the implementation of chip-and-PIN systems. At the Subcommittee hearing on February 5, 2014 – while stressing that the Commission does not recommend any particular technology – you indicated that "we would support any steps that are taken at the payment card system end to protect or better protect consumer information." I believe it is important for retailers, issuers, and the payment card industry to urgently work together to improve card security. However, even if all the stakeholders involved agree to make payment card data as secure as possible, am I correct to understand that it is your position that that Congress should still separately address the overall security of personal data, including non-financial data, collected or stored by commercial entities?

That is correct. The Commission is aware of this developing technology, and according to some reports, it should be a positive step toward strengthening payment card security. However, this technology does not protect other information, such as health information, location information, or SSNs.

All companies that collect and handle consumer information should be required to implement reasonable data security measures. Reasonableness is the appropriate standard because it allows a company flexibility to develop a data security program based on factors such as the sensitivity and volume of consumer information it holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

The Commission reiterates our call for data security and breach notification legislation that would: (1) give us the authority to obtain civil penalties, an important remedy for deterring violations; (2) enable the FTC to bring cases against non-profits, such as hospitals and educational institutions, where many breaches occur; and (3) providing rulemaking authority under the Administrative Procedure Act, enabling the FTC to respond to changes in technology when implementing the legislation.

I believe the breach of marketing data can be a serious threat to consumers. As I said in response to questioning at the Subcommittee's hearing, names and contact information can be used in phishing and social engineering schemes to try to perpetrate identity theft – and while harm from payment card breaches tends to be acute, harm from non-financial breaches tends to linger. In short, identity theft lasts; with chronic effects on consumers that can cost them everything they own.

c. Do you agree that a breach of names and contact information can have a serious long-term impact on consumers, if used to trick them to give up sensitive identity data? Please explain your answer.

Yes. As discussed above, such information can be used to perpetrate fraud and identity theft, which can have lasting impacts on consumers' credit scores, in addition to the economic value of time lost and possible financial loss.

2. On January 31, 2014, the FTC announced the 50th data security settlement in its program of enforcement against those who fail to reasonably protect consumers' personal information. These settlements have been used to protect millions of consumers from unfair or deceptive practices that leave at risk sensitive information like usernames and passwords, Social Security numbers, and health, financial, and children's data. I commend your dedication to this issue.

   Yet, during questioning at the Senate Banking Committee hearing on this topic on February 3, 2014, a Senator pointed out that with so many data breaches each year, 50 cases since 2002 may be commendable, but it may not be enough.

   a. Of course, all breaches do not rise to the level of FTC action, but can you please illustrate how the FTC uses its current legal framework to help with general deterrence, and how authorization to the FTC of new authorities, such as rulemaking authority under the Administrative Procedure Act and broader civil penalty authority, would increase the FTC's ability to deter unfair or deceptive data security practices?

Since 2002, the FTC has brought a steady stream of data security cases – resulting in more than 50 consent orders, and we have also issued extensive consumer and business education materials. During much of this time, we have been the only federal agency sending the message to a wide range of businesses, both small and large, across many sectors, of the need to maintain reasonable security to protect consumer data. Our complaints provide examples of data security practices that did not meet our flexible reasonableness test, and our consent orders serve as templates for best practices for companies setting up and implementing successful information security programs. In addition, we issue extensive guidance for consumers and businesses – especially small businesses – about how to safeguard consumer data. I believe that collectively the FTC's work in this area has helped promote appropriate investment in infrastructure and personnel to address the security of consumer data.

But, plainly, more needs to be done, and a unanimous Commission has concluded that the time has come for Congress to enact strong federal data security and breach notification legislation. We currently lack authority under Section 5 to obtain civil penalties, which are critical to appropriate deterrence of lax security practices. Likewise, enabling the FTC to bring cases against non-profits, over which we presently lack authority, would help ensure that whenever personal information is collected from consumers, the entities that maintain such data take reasonable measures to protect it. Finally, APA rulemaking would give us flexibility in implementing the statute by

making changes where appropriate – for example, to the definitions – to respond to changes in technology and changing threats.

b. Recent newspaper commentary has suggested that by seeking to strengthen its data security authority, the FTC is acknowledging that it currently lacks the authority to police companies' data security practices. How do you respond to such an assertion?

The Commission principally has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle over 50 data security cases to date. In fact, a federal district court recently affirmed the FTC's authority to use Section 5 in the data security area.[5]

The Commission has called for data security legislation that would strengthen its existing tools and authority to help us in this endeavor, namely, civil penalty authority, jurisdiction over non-profits, a nationwide breach notice requirement to be enforced by the FTC and the states, and APA rulemaking to ensure we have adequate flexibility to respond to new technology and threats in implementing the statute.

The Honorable Jerry McNerney

1. Thank you for your leadership within the FTC, especially with regards to the work that is being done on privacy issues. What sort of authority does the Commission have or need from Congress to institute nationwide breach notification processes?

The FTC has authority to investigate breaches and bring civil enforcement actions under Section 5 of the FTC Act for deceptive or unfair acts or practices – such as deceptively claiming to reasonably safeguard consumer data. We have authority to seek equitable remedies for violations of Section 5, which does not include civil penalties.[6] The FTC also generally lacks authority to require companies to issue notification to affected consumers to alert them to a breach of their personal information (with the exception of our narrow scope of authority under the HI-TECH Act). We similarly lack authority over non-profits, which have been the source of a number of breaches. To remedy these gaps, a unanimous Commission has called on Congress to enact legislation to pass a nationwide breach notification law to apply to all companies under the FTC's jurisdiction – expanding that jurisdiction to include non-profits –and to give the Commission civil penalty authority and authority to flexibly respond to changes in technology in implementing the law via APA rulemaking.

2. Businesses are understandably leery of the idea of additional regulations, but many people that I have talked with agree that a national standard is easier to deal with than varying state standards when it comes to data breach notification rules. In your opinion, how can the FTC

[5] *See F.T.C. v. Wyndham Worldwide Corp*, No. 2:13-cv-01887-ES-JAD, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *petition for leave to appeal filed* (3d Cir. July 3, 2014).

[6] By contrast, the FTC has civil penalty authority under the Fair Credit Reporting Act for security violations by "consumer reporting agencies," such as the national credit bureaus.

and Congress best work together to come up with a national standard that doesn't impose unfairly upon states' rights?

Breach notification and data security standards at the federal level, with appropriate preemption of state law as discussed below, would extend notifications to all citizens nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A federal law would create uniform protections for all American consumers. However, our support for a federal law that would preempt state law has been conditioned on both a standard that is sufficiently strong and on giving states the ability to enforce the law, an important role for state Attorneys General.

The Honorable Peter Welch

1. We've seen the FTC take a strong leadership position on many issues, not only bringing enforcement actions but also convening experts from industry and academia at workshops. These workshops have been valuable opportunities for the FTC to write reports on what it learns, including guidance to companies when appropriate. It seems to me like an annual workshop and report on data security would be valuable given the recent problems companies have been having -- can we expect the FTC to have such a workshop soon?

   Thank you for your recognition of the FTC's leadership on many issues and the value of our use of enforcement actions and public workshops. As you may know, emerging areas in privacy and security are frequent subjects of FTC workshops, studies, and reports. For instance, in June of last year, we held a workshop on threats to mobile security, in which we convened a group of leading experts to discuss mobile malware, the role of platforms in security, and ways to improve security in the mobile ecosystem.[7] Earlier this year, the FTC hosted a "Spring Privacy Series" to examine the privacy and security implications of a number of new technologies in the marketplace, including mobile device tracking, alternative scoring products, and apps and devices that collect consumer-generated health data.[8] At the Commission's November 2013 conference on the Internet of Things, much of the discussion focused on security challenges presented by "smart" devices.[9]

   Moreover, the FTC just published its first annual "Privacy and Data Security Update," which is an overview of the FTC's enforcement, policy initiatives, and consumer

---

[7] *See* Mobile Security: Potential Threats and Solutions (June 4, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions.

[8] *See* FTC to Host Spring Seminars on Emerging Consumer Privacy Issues, *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues.

[9] *See* Internet of Things - Privacy and Security in a Connected World (Nov. 19, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

outreach and business guidance in the areas of privacy and data security from January 2013-March 2014.[10] We expect to update this document every year.

[10] Federal Trade Commission Staff, 2014 Privacy and Security Update (June 2014), *available at* http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

Kelly, Andrea

From: Taylor, Shannon <shannon.taylor@mail.house.gov>
Sent: Wednesday, June 18, 2014 12:16 PM
To: Vandecar, Kim
Subject: LabMD/Tiversa/Government Reform

Follow Up Flag: Follow up
Flag Status: Flagged

Hey, Kim.

I've been meaning to reach out to you on this. You guys have any thoughts you want to share with us, or just tell us generally what's happening in this case now that Government Reform is sniffing around Tiversa?

http://blogs.wsj.com/riskandcompliance/2014/06/03/u-s-lawmakers-investigating-ftcs-use-of-firm-in-data-cases/

http://blogs.wsj.com/riskandcompliance/2014/06/12/house-committee-says-ftc-privacy-case-incomplete-and-inaccurate/

Shannon Taylor
Counsel, Majority Staff
Committee on Energy & Commerce
U.S. House of Representatives
2125 Rayburn HOB/316 Ford HOB
Washington, DC 20515
202.225.2927