

KING & SPALDING

King & Spalding LLP
1700 Pennsylvania Ave, NW
Washington, D.C. 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
www.kslaw.com

Theodore M. Hester
Direct Dial: 202-626-2901
thester@kslaw.com

VIA E-MAIL

September 28, 2017

The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

RE: Equifax's Submission in Response to Committee Requests Dated Sept. 12, 2017

Dear Ranking Member Pallone:

On behalf of our client, Equifax Inc. ("Equifax"), I am writing in response to your September 12, 2017 letter regarding the recent Equifax cybersecurity incident. After receiving your recent letter, Equifax briefed Committee on Energy and Commerce staff on September 19, 2017, providing as much detail as possible in light of Equifax's ongoing investigation. To further your understanding of this incident, Equifax also provided Committee staff with certain summary information and answered questions to the extent possible at this time.

Pursuant to discussions with Committee staff, Equifax has asked me to formally submit the enclosed information, responsive to your requests, attached as Appendix A to this letter. Equifax has also asked me to provide copies of the executive summary report, along with the related supplemental report, provided to Equifax by the independent cybersecurity firm, Mandiant. We will supplement today's submission as additional information becomes available. We appreciate the additional time for Equifax to respond to your letter with rolling submissions.

In responding to your requests, Equifax has used its best efforts to be as accurate and responsive as possible based on its understanding of the terms used in your letter. The representations herein are based on reasonably available information and are not intended to and do not capture every event related to Equifax's ongoing investigation, nor are they an exhaustive description of the events discussed. In providing these responses, Equifax does not waive, nor does it intend to waive, any of its rights or privileges with respect to this inquiry, including any applicable attorney-client, work product or other evidentiary privilege, or any objections to the assertions or requests in your letter.

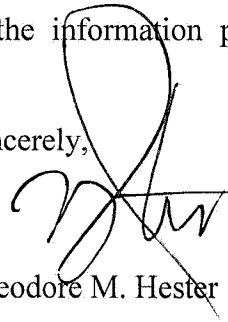
The Honorable Frank Pallone, Jr.

September 28, 2017

Page 2

Should you have any questions concerning the information provided herein, please contact me directly at 202-626-2901.

Sincerely,

A handwritten signature in black ink, appearing to read 'Theodore M. Hester', written over a horizontal line.

Theodore M. Hester

cc: Ranking Member Bobby L. Rush,
Subcommittee on Energy

Ranking Member Gene Green,
Subcommittee on Health

Ranking Member Diana DeGette,
Subcommittee on Oversight and Investigations

Ranking Member Mike Doyle,
Subcommittee on Communications and Technology

Ranking Member Jan Schakowsky,
Subcommittee on Digital Commerce and Consumer Protection

Ranking Member Paul D. Tonko,
Subcommittee on Environment

Vice Ranking Member Kathy Castor,
Committee on Energy and Commerce

Anna G. Eshoo, Member

Eliot L. Engel, Member

G.K. Butterfield, Member

Doris O. Matsui, Member

John Sarbanes, Member

Jerry McNerney, Member

Peter Welch, Member

Ben Ray Luján, Member

Yvette D. Clarke, Member

Dave Loebsack, Member

Kurt Schrader, Member

Joseph P. Kennedy, III, Member

Enclosures

Appendix A

EQUIFAX'S SUBMISSION IN RESPONSE TO REQUESTS DATED SEPTEMBER 12, 2017

Request #1, 2, 3, and 5.

Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, along with a related supplemental report. Mandiant's investigation is ongoing. For your reference, we are providing the executive summary and the supplemental report again today.

Equifax conducts regular security reviews and it participates in various certification programs.

Request #4. This breach is the third that Equifax has experienced in two years. What changes to its data security plans and procedures did Equifax make following each of the two previous data breaches?

Request 4 appears to reference two fraud incidents experienced by TALX Corporation, a wholly-owned subsidiary of Equifax. TALX Corporation, operating under the trade name Equifax Workforce Solutions, provides human resources, payroll, tax management, and compliance services. These fraud incidents were not related to the recent cybersecurity incident (see, in pertinent part, Mandiant's supplemental report). A brief background summary of these fraud incidents follows:

- TALX experienced fraud incidents during Spring 2016 and Spring 2017.
- During the Spring of 2016, fraudsters used personal information obtained from non-Equifax sources to access employee accounts that used personally identifiable information for the user ID (e.g., Social Security numbers) and personal information for the related default PIN (e.g., the last four digits of a Social Security number or a year of birth). In response to the 2016 unauthorized access, TALX added an additional layer of authentication for the 2017 tax season so that no individual could log into the system using a default PIN containing personally identifiable information. The revised process included knowledge-based authentication ("KBA").
- During the Spring of 2017, TALX received reports of unauthorized access to individuals' W-2s contained within TALX's online platform. This incident did not involve any hacking of Equifax systems, and there was no mass exfiltration of data. While TALX was combatting these fraud cases in 2017, TALX made modifications to the KBA configuration in order to make it more difficult to pass. On a moving forward basis, TALX is continuing to modify its authentication protocol.

- The fraud incidents involving TALX are different from and unrelated to the recently announced cybersecurity incident. Equifax is not aware of any evidence that the recent cybersecurity incident attacker accessed Equifax's The Work Number database.

Request #6. Equifax's press release notes that the "information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers," but that for some consumers, credit card numbers and "certain dispute documents with personal identifying information ... were accessed." What specific dispute documents were accessed in this breach? What other personal identifying information was compromised?

The dispute documents accessed in this breach are documents that individuals uploaded to Equifax's online credit report consumer dispute portal between approximately January 1, 2013 and July 22, 2017. As a national credit reporting agency, Equifax has a statutory obligation to facilitate disputes between consumers and their creditors. The documents at issue were documents that individuals presented as evidence in support of a credit report dispute with their creditors. Such documents may contain sensitive personal information in addition to those data elements listed above (name, address, birthdate, and social security number).

Request #7, 8, 14-16.

Equifax rolled out a support package to consumers on September 7, 2017, which included a free credit file monitoring and identity theft protection to all U.S. consumers, regardless of whether they were definitively impacted. TrustedID Premier includes: (1) three-Bureau credit monitoring of Equifax, Experian, and TransUnion credit reports; (2) copies of Equifax credit reports; (3) the ability to lock and unlock Equifax credit reports; (4) identity theft insurance; and (5) Internet scanning for Social Security numbers.

Last night, the Wall Street Journal published an op-ed by Equifax's Interim Chief Executive Officer, Paulino do Rego Barros, Jr., outlining what credit monitoring and other consumer protection services Equifax believes will be effective protecting consumers going forward (emphasis added)¹:

On behalf of Equifax, I want to express my sincere and total apology to every consumer affected by our recent data breach. People across the country and around the world, including our friends and family members, put their trust in our company. We didn't live up to expectations.

We were hacked. That's the simple fact. But we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to

¹ <https://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253>

key consumer questions were too often delayed, incomplete or both. We know it's our job to earn back your trust.

We will act quickly and forcefully to correct our mistakes, while simultaneously developing a new approach to protecting consumer data. In the near term, our responsibility is to provide timely, reassuring support to every affected consumer. ***Our longer-term plan is to give consumers the power to protect and control access to their personal credit data.***

I was appointed Equifax's interim chief executive officer on Tuesday. I won't pretend to have figured out all the answers in two days. But I have been listening carefully to consumers and critics. I have heard the frustration and fear. I know we have to do a better job of helping you.

Although we have made mistakes, we have successfully managed a tremendous volume of calls and clicks. And we're getting better each day. But it's not enough. I've told our team we have to do whatever it takes to upgrade the website and improve the call centers.

We have started work on our website, and I see significant signs of progress. I won't accept anything less than a superior process for consumers. We will make this site right or we will build another one from scratch. You have my word.

The same goes for the call centers. There is no excuse for delayed calls or agents who can't answer key questions. We will add agents and expand training until calls are answered promptly and knowledgeably. I will personally review a daily report on their operations.

We will also extend the services we are offering consumers. We have heard your concern that the window to sign up for free credit freezes with Equifax is too brief, so we are extending the deadline to the end of January. Likewise, we are extending the sign-up period for TrustedID Premier, the complimentary package we are offering all U.S. consumers, through the end of January.

We hope these immediate actions will go a long way toward addressing the concerns we are hearing from consumers. We know they won't solve the larger problem. We have to see this breach as a turning point—not just for Equifax, but for everyone interested in protecting personal data. Consumers need the power to control access to personal data.

Critics will say we are late to the party. But we have been studying and developing a potential solution for some time, as have others. Now it is time to act.

So here is our commitment: By Jan. 31, Equifax will offer a new service allowing all consumers the option of controlling access to their personal credit data. The service we are developing will let consumers easily lock and unlock access to their Equifax credit files. You will be able to do this at will. It will be

reliable, safe and simple. Most significantly, the service will be offered free, for life.

With the extension of the complimentary TrustedID package and free credit freezes into the new year, combined with the introduction of this new service by the end of January, we will be able to offer consumers both short- and long-term support for their personal data security.

There is no magic cure for data breaches. As we all know, every organization is at risk. When consumers have access to our new service, however, the cybercrime business will become a lot more difficult, and we are committed to doing what we can to help millions of consumers rest easier.

Request #9. What federal and state officials has Equifax notified of the data breach? When did Equifax notify these officials? It is our understanding that consumers in the United Kingdom and Canada were also affected by this breach. When and how were those consumers and government officials notified?

On September 7, 2017, Equifax notified the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), and the attorneys general or equivalent consumer protection agencies for 52 states and territories regarding the cybersecurity incident.

Equifax has also notified the appropriate regulatory agencies in the United Kingdom and Canada and will provide notice to affected consumers in consultation with those agencies.

Request #10. Bloomberg has reported that three senior executives of Equifax “sold shares worth almost \$1.8 million” on August 1, 2017—just days after the company discovered the breach on July 29, 2017. What measures is the company taking to investigate the sale of stock in the aftermath of the company’s discovery of the data breach, including whether these or other executives sought to delay the announcement of the data breach? What date did these officials find out that there was a breach?

Equifax takes these matters seriously. The Board of Directors has formed a Special Committee. The Committee has retained counsel and is conducting a thorough review of the trading at issue.

Request #11. What procedures does Equifax have in place for notifying senior officers within the company in the event of a data breach? Did Equifax comply with those procedures in this case? Are senior officials notified of every unauthorized access or unauthorized acquisition of company or consumer information? At what point are they notified?

- Equifax has several plans and procedure guides that address cybersecurity incidents.
 - Equifax’s Security Incident Handling Procedure Guide establishes procedures for identifying, classifying, and responding to cybersecurity incidents.

- Equifax’s Security Incident Response Team Plan (“SIRT Plan”) defines principles, roles, and responsibilities for team members who support cybersecurity and other aspects of Equifax’s incident response program.
- Equifax’s Security and Safety Crisis Action Team Plan (“CAT Plan”) is used in tandem with the Crisis Management Plan, and addresses circumstances that have been “declared a corporate incident or a corporate crisis” by the Crisis Management Team.
- Equifax faces numerous cyber threats every day. Its Cyber Threat Center (“CTC”) constantly assesses whether a particular threat can be resolved quickly by the Company’s own internal cybersecurity team, or whether the threat will require additional resources to remediate. If the CTC determines that a cybersecurity threat is unusual and will require additional resources to contain, it is typically designated a “Security Incident” and Equifax’s Incident Guide is triggered.
- As set forth in the Incident Guide, once a Security Incident has been declared, its severity is classified based on a risk assessment including:
 - number of affected systems;
 - network impact;
 - business services impact;
 - sensitivity of information threatened or compromised; and
 - the potential for harm.
- Various senior officers, including those within the Legal Department, are notified by security of Security Incidents and typically outside experts are retained (e.g., a forensic team and outside counsel) to assist with the response.
- There is an ongoing root cause investigation into multiple issues, including compliance with Equifax’s plans and procedure guides.

Request #13. To sign up for TrustedID Premier, Equifax’s credit monitoring service and identify theft protection offered to consumers in connection with this breach, a consumer must agree to the TrustedID Premier terms of use, which initially included an arbitration clause—language that New York Attorney General Eric Schneiderman called “unacceptable and unenforceable.” How did Equifax arrive at the decision to include an arbitration clause in its product’s terms of use? After first attempting to clarify that “the arbitration clause and class action waiver included in the Equifax and TrustedID Premier terms of use does not apply to this cybersecurity incident,” Equifax ultimately removed the arbitration language from its TrustedID Premier terms of use. However, the arbitration clause in Equifax’s general terms of use on its website remains. Will Equifax attempt to enforce this or any other arbitration clause against consumers who choose to use the TrustedID Premier service or consumers affected by the data breach, including those affected consumers who had previously purchased or subscribed to an Equifax product?

Equifax has addressed confusion concerning the arbitration and class-action waiver clauses initially included in the Terms of Use applicable to TrustedID products. To be clear, Equifax never intended for these clauses to apply to this cybersecurity incident. Due to consumer concern, the company clarified that those clauses do not apply to this cybersecurity incident or to the complimentary TrustedID Premier offering. The company clarified that the clauses will not apply to consumers who signed up before the language was removed. Equifax has updated the Terms of Use and the www.equifaxsecurity2017.com website to reflect this point.