GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

September 12, 2017

Richard F. Smith
Chairman and CEO, Equifax Inc.
1550 Peachtree Street NE
Atlanta, GA 30309

Dear Mr. Smith:

Equifax announced on Thursday, September 7, 2017, that hackers had compromised the sensitive personal data—including Social Security Numbers, birth dates, names, addresses and other information—of "approximately 143 million U.S. consumers."[1] This announcement came more than a month after the company discovered the data breach on July 29, 2017, and nearly four months after the unauthorized access first occurred.[2]

Equifax's public announcement of the breach directed consumers to the website equifaxsecurity2017.com. Almost immediately, reports surfaced of a number of problems with the website.[3] Some browsers were flagging the website as a phishing scam.[4] Consumers reported that to find out if their information was compromised, the website requested two-thirds of people's Social Security numbers in combination with their last names.[5] And even after providing that information, the status of their personal information is unclear or misleading.[6] People who checked the website on both their mobile device and a computer received different

---

[1] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017) (press release).

[2] *Id.*

[3] *Equifax Breach Response Turns Dumpster Fire*, Krebs on Security (Sept. 8, 2017) (krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/).

[4] *Id.*

[5] *Id.*

[6] *Id.*

results.[7] And false information entered into the fields provides the same result as real information.[8]

We are writing with serious concerns about the immense scale of this data breach, and we have a number of questions about whether Equifax took appropriate steps to safeguard the personal information of consumers. We also have concerns about the amount of time it took for Equifax to notify the public of the breach and about the way Equifax is providing information to consumers.

In order to access credit, and to participate in the modern economy, American consumers have virtually no choice but to entrust their sensitive personal information to the three main credit bureaus, including your company. Consumers cannot avoid sharing their personal information with your company by simply choosing to transact business elsewhere, and many consumers may be unaware that your company actually has their personal information. It is critical for companies like yours to protect consumer data, and to inform consumers when those protections fail.

We seek answers to the following questions about what actions the company is taking to make consumers whole, how the breach occurred, and what the company is doing to safeguard against security breaches in the future:

1. Equifax's press release stated that criminals exploited a "website application vulnerability to gain access to certain files."[9] What was the specific vulnerability that was exploited? What is Equifax doing to identify other weaknesses in its data security program? Does the company conduct regular security audits? If so, how often? Please explain in detail the process for any such security audits.

2. What security controls were in place that failed to protect sensitive consumer information? How recently were these security controls audited? How were the criminals able to conduct the exfiltration of consumer data by exploiting the website vulnerability?

3. Why were the Equifax network operations and security staff unaware that volumes of data involving 143 million U.S. consumers had been exfiltrated from the Equifax network for so long? Does Equifax regularly monitor for intrusions into its network? Was it conducting regular monitoring during the time of the breach?

---

[7] *Id.*

[8] *Id.*

[9] *Id.*

4. This breach is the third that Equifax has experienced in two years.[10] What changes to its data security plans and procedures did Equifax make following each of the two previous data breaches?

5. What operational and technical measures is Equifax implementing after the event to improve the protection of consumer information residing on its network?

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."[11] What specific dispute documents were accessed in this breach? What other personal identifying information was compromised?

7. Why did it take Equifax more than a month to announce this massive data breach? What specific actions did Equifax take in this time to protect consumer information and mitigate potential harms to consumers resulting from the breach?

8. What is Equifax doing to notify individual consumers whose information was compromised in the data breach? According to Equifax's press release, the company will directly notify consumers "whose credit card numbers or dispute documents with personal identifying information were impacted."[12] Does this mean that Equifax will directly notify only a portion of the 143 million consumers whose personal information was compromised?

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?

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.[13] What measures is the company taking to investigate the sale of stock in the aftermath of the company's discovery of the data breach,

---

[10] *How to Find Out if You're Affected by the Massive Equifax Cyberattack*, BGR (Sept. 8, 2017) (bgr.com/2017/09/08/Equifax-personal-data-hack-how-to-find-out/).

[11] *See* note 1.

[12] *Id.*

[13] *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, Bloomberg (Sept. 7, 2017) (www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack).

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?

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?

12. Equifax provides credit monitoring services to companies whose customers have been affected by data breaches. In this case, the very company whose data was breached is itself providing its own customers with credit monitoring services. Equifax's press release states that the company will provide affected consumers with credit monitoring services and identity theft protection "complimentary to U.S. consumers for one year."[14]

    a. What analysis did the company do to determine that one year of complimentary credit monitoring services and identity theft protection—provided by Equifax itself—would be adequate to make consumers whole? How does this service differ from the Equifax product known as Equifax ID Patrol and other services sold as part of Equifax's regular business?

    b. How much money per year would an affected consumer who received this free service pay Equifax to extend the "complimentary" services beyond one year?

    c. Has Equifax estimated how much money it would make per year if every one of the 143 million consumers affected by Equifax's data breach signed up for Equifax's credit monitoring service and identity theft protection? In short, how much money would Equifax make after one year on credit monitoring services that would be unnecessary but for Equifax's failure to safeguard consumer data?

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."[15] How did Equifax arrive at the decision to include an arbitration clause in its product's terms of use? After first attempting to

---

[14] *See* note 1.

[15] Equifax, *TrustedID Premier Terms of Use* (Sept. 6, 2017) (trustedidpremier.com/static/terms); *By Signing Up On Equifax's Help Site, You Risk Giving Up Your Legal Rights*, Washington Post (Sept. 8, 2017) (www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm_term=.3849838f08a2).

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.[16] However, the arbitration clause in Equifax's general terms of use on its website remains.[17] 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?

14. What measures, other than offering credit monitoring services and identity theft protection, is Equifax taking to mitigate harm to consumers?

15. Will Equifax waive fees associated with consumers' freezing their credit with Equifax? Will Equifax pay for consumers affected by the breach to freeze their credit with the other credit bureaus?

16. Finally, at the request of members of the Energy and Commerce Committee, the Government Accountability Office is evaluating the effectiveness of credit monitoring and other services in protecting consumers after a data breach.[18] What analysis has Equifax done to determine whether its monitoring services and identity theft protection, both offered for free in the wake of this breach or sold as a regular product, are effective in preventing identity theft or otherwise protecting consumers after a data breach?

Your company profits from collecting highly sensitive personal information from American consumers—it should take seriously its responsibility to keep data safe and to inform consumers when its protections fail. Your assistance in this matter is greatly appreciated, and we look forward to receiving a response by September 22, 2017. Answers to these questions will also help us prepare for a Committee hearing on this issue that is planned for either later this month or in October.

---

[16] *Consumer Backlash Spurs Equifax to Drop 'Ripoff Clause' In Offer to Security Hack Victims*, Forbes (Sept. 9, 2017) (www.forbes.com/sites/dianahembree/2017/09/09/consumer-anger-over-equifaxs-ripoff-clause-in-offer-to-security-hack-victims-spurs-policy-change/#69a83c226e7e).

[17] Equifax, *Equifax Terms of Use* (May 2, 2015) (www.equifax.com/terms/).

[18] House Committee on Energy and Commerce, *E&C Dem Leaders Ask GAO to Evaluate Effectiveness of Post-Breach Services in Protecting Consumer Data* (Aug. 30, 2017) (press release).

If you have any questions, please contact the Democratic Committee staff of the House Energy and Commerce Committee at (202) 225-3641.

Sincerely,

Frank Pallone, Jr.
Ranking Member

Bobby L. Rush
Ranking Member
Subcommittee on Energy

Anna G. Eshoo
Member of Congress

Eliot L. Engel
Member of Congress

Gene Green
Ranking Member
Subcommittee on Health

Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations

Mike Doyle
Ranking Member
Subcommittee on Communications
and Technology

Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection

G.K. Butterfield
Member of Congress

Doris O. Matsui
Member of Congress

Kathy Castor
Vice Ranking Member
Committee on Energy and Commerce

John Sarbanes
Member of Congress

Jerry McNerney
Member of Congress

Peter Welch
Member of Congress

Ben Ray Luján
Member of Congress

Paul D. Tonko
Ranking Member
Subcommittee on Environment

Yvette D. Clarke
Member of Congress

Dave Loebsack
Member of Congress

Kurt Schrader
Member of Congress

Joseph P. Kennedy, III
Member of Congress

Tony Cárdenas
Member of Congress

Raul Ruiz, M.D.
Member of Congress

Scott H. Peters
Member of Congress

Debbie Dingell
Member of Congress

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu