ELIZABETH WARREN
MASSACHUSETTS

COMMITTEES:
BANKING, HOUSING, AND URBAN AFFAIRS
HEALTH, EDUCATION, LABOR, AND PENSIONS
ARMED SERVICES
SPECIAL COMMITTEE ON AGING

United States Senate

UNITED STATES SENATE
WASHINGTON, DC 20510–2105
P: 202–224–4543

2400 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
P: 617–565–3170

1550 MAIN STREET
SUITE 406
SPRINGFIELD, MA 01103
P: 413–788–2690

www.warren.senate.gov

September 15, 2017

Richard F. Smith
Chairman and Chief Executive Officer
Equifax
1550 Peachtree St. NE
Atlanta, GA 30309

Dear Mr. Smith:

I write regarding last week's announcement of the massive breach that allowed criminal hackers access to sensitive personal information – including Social Security numbers, birth dates, credit card numbers, and driver's license numbers – potentially impacting over 140 million Americans. Today I am opening a broad investigation into the causes of the breach and the response by Equifax. I am also introducing legislation to provide consumers with free credit freezes. Finally, I am writing to other credit rating agencies, to federal regulators, and to GAO to obtain information needed to determine if broader federal legislation is necessary to further protect consumers.

I am troubled by this attack – described as "one of the largest risks to personally sensitive information in recent years" – and by the fact that it represents the third recent instance of a data breach of Equifax or its subsidiaries that has endangered American's personal information.[1] And I have deep concerns about the initial response by Equifax.

According to a statement released by your company, Equifax first "discovered the unauthorized access on July 29," but the company did not make any public announcement until 40 days later, on September 7, 2017.[2] The breach has put "really sensitive" data of four in ten Americans at risk, in what "has the potential to be a very harmful breach to those who are affected by it."[3] Americans impacted by the hack are at risk of becoming victims of credit card fraud, tax fraud, identity theft, and various other crimes.[4] Given the risk to so many Americans, it is unclear why you delayed in notifying them of any breach.

---

[1] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, & Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *New York Times*, Sept. 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.
[2] Equifax, "Equifax Announces Cybersecurity Incident Involving Consumer Information," press release, Sept. 7, 2017, https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.
[3] Craig Timberg, Elizabeth Dwoskin, & Brian Fung, "Data of 143 million Americans exposed in hack of credit reporting agency Equifax," *Washington Post*, Sept. 7, 2017, https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html.
[4] Seena Gressin, "The Equifax Data Breach: What to Do," Federal Trade Commission, Consumer Information blog, Sept. 8, 2017, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

The announcement also failed to provide clarity on what precise information was accessed by the hackers, and how it was done. In order to address this issue and ensure that Americans' data are safe in the future, we must understand exactly what failures allowed hackers to gain access to nearly 150 million Americans' sensitive data. Equifax has failed to provide the necessary information describing exactly how this happened, and exactly how your security systems failed.

Furthermore, Equifax's initial efforts to provide customers information did nothing to clarify the situation and actually appeared to be efforts to hoodwink them into waiving important legal rights. Equifax's website provides a "Potential Impact" feature that asks consumers for their name and the last six digits of their social security numbers – the same sensitive information Equifax already failed to protect – and promises to send consumers "a message indicating whether your personal information may have been impacted by this incident." Yet according to the New York Times, Equifax provided consumers no new useful information about data even when they followed the prescribed steps; according to the Times, entering a random set of names and numbers led to the exact same unclear and imprecise message as entering actual identifying information – the unhelpful response that "your personal information may have been impacted by this incident."[5]

Rather than giving consumers useful information regarding the breach's potential impact, Equifax's service instead offered one free year of "TrustedID Premier," Equifax's pay-for credit monitoring service. This offer concerns me for a number of reasons.

First, the service will do nothing to protect Americans from hackers who use their information "to apply for credit with lenders that check the credit reports" at other agencies besides Equifax, a fact that is not readily provided to potential consumers. In addition, in the first few days after the announcement of the breach, the Equifax credit monitoring offer appeared to expire after one year, at which point Equifax stated that the company would begin automatically begin billing customers unless they affirmatively cancel the service.[6]

Perhaps worst of all, in order to sign up for the free credit monitoring service Equifax initially appeared to force consumers to give up their rights to go to court and sue Equifax if they have disputes about the credit monitoring service in the future. Equifax modified this requirement after public outcry; but it is unconscionable that after putting consumers' data at risk, Equifax seemed to be trying to strip consumers of their rights by requiring them to agree to binding arbitration of future disputes in order to obtain partial protection from the consequences of a hack that Equifax was responsible for preventing.

To address these concerns and provide the public with clarity on the causes of and extent of the breach, I ask that you answer the following questions no later than [two weeks]. I understand that you have similar inquiries from other members and committees, and I understand that some of my

---

[5] Ron Lieber, "Equifax's Instructions Are Confusing. Here's What to Do Now," *New York Times*, Sept. 8, 2017, https://www.nytimes.com/2017/09/08/your-money/identity-theft/equifaxs-instructions-are-confusing-heres-what-to-do-now.html.

[6] Paul Blumenthal & Arthur Delaney, "Equifax Is Trying To Make Money Off Its Massive Security Failure," *Huffington Post*, Sept. 8, 2017, http://www.huffingtonpost.com/entry/equifax-breach-2017_us_59b2dae8e4b0b5e531062976?746.

questions concern information that may be confidential, and am happy to discuss this matter with you to address any concerns and ensure that business- or law enforcement-sensitive and important confidential information is not made public.

1. How did Equifax discover the breach, and what information did the company receive that resulted in the discovery? When did company officials receive this initial information, and how long did it take to ultimately "discover" the breach after receipt of this initial information?

2. How is Equifax informing customers if their individual data has been exposed? Is the company affirmatively sending letters or otherwise contacting customers, or is Equifax requiring that customers go to the company website to obtain information?

3. Precisely what was the extent of the breach?

    a. How many U.S. individuals' Social Security numbers were accessed?
    b. How many U.S. individuals' birth dates were accessed?
    c. How many U.S. individuals' driver's license numbers were accessed?
    d. Your press release indicates that "certain dispute documents with personal identifying information" were accessed for 182,000 U.S. customers. Exactly what kind of documents were accessed?
    e. Were any other kinds of document or information accessed besides names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and "certain dispute documents"? If yes, what type of documents, and how many U.S. consumers were affected?

4. Your press release indicates that "the company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases."

    a. What does this statement mean? What are Equifax's "core consumer or commercial credit reporting databases" and how are they distinct from other databases containing personal information maintained by Equifax?
    b. Which company databases were accessed by the hackers?
    c. What is their function, and why are they not considered to be part of Equifax's "core consumer or commercial credit reporting databases"?

5. Equifax holds dozens of federal contracts for data services at a number of key federal agencies.[7] Was any data related to or maintained under these contracts compromised? If so, please describe which contracts and which data was compromised.

6. Why did it take Equifax 40 days to notify the public of the breach? Please provide a timeline of all key breach-related activity by Equifax and Equifax agents and representatives between

[7] Advanced data search on USAspending.gov, https://www.usaspending.gov/Pages/AdvancedSearch.aspx?sub=y&ST=C,G,L,O&FY=2017,2016,2015,2014,2013,2012,2011,2010,2009,2008&A=0&SS=USA&k=equifax&pidx=2&SB=RN&SD=ASC.

July 29 and September 7, and a timeline of when key company executives and board members were informed of the breach, how they were informed, and what action they took in responses.

7. Has any company executive been fired or otherwise penalized as a result of the breach? If so, please provide details on these executives and their punishment.

8. Did Equifax inform any of its regulators of the breach before informing the public? If so, please describe the communications and the timeline of communications.

9. Please describe all actions taken by Equifax to identify the root cause of the breach. What conclusions has Equifax reached with regards to the root cause of the breach, and what actions has the company taken in response to these findings? Is Equifax collaborating with any law enforcement agencies to determine the source of the breach?

10. Was the root cause of the breach related in any way to the previous hacks that resulted in the theft of W-2 tax and salary data from Equifax in 2016, or the theft of W-2 tax data from Equifax subsidiary TALX earlier this year? Does Equifax know of any other data breaches it had not reported publicly?

11. Were all key web applications and other software used by Equifax to prevent data breaches updated with the most recent security patches at the time of the breach? If not, which web applications were not updated?

12. Has Equifax identified the hackers responsible for the breach, and their country of origin? If so, who were the hackers, and what was their country of origin? Is there any reason to believe that the hackers were working with or for a hostile nation-state or a terrorist organization?

    a. Did Equifax, after these two earlier attacks, conduct a root cause analysis and develop or obtain a set of recommendations to prevent future breaches?
    b. If so, please provide a summary of these recommendations.
    c. If so, were they fully implemented at the time of the July 2017 breach?

13. Prior to July 29, 2017 did Equifax have a plan in place to respond to a large-scale security breach?

    a. If so, please provide a copy of this plan.
    b. If so, was this plan followed in its entirely following the July 2017 breach? If not, where did the Equifax response deviate from this plan, and why?

14. Why did Equifax initially include a requirement that consumers consent to arbitration (giving up their right to go to court to redress grievances) in order for consumers to determine whether their data has been breached? Does Equifax require consumers to consent to arbitration with respect to any of its other products?

15. The New York Times reported that consumers were unable to determine with certainty if their information was breached, reporting that the Equifax site for consumers indicated – in response to all inquiries – that personal information "may have" been compromised. Why was Equifax unable to provide clarity on whether individuals' information was breached?

16. Your website directs consumers to sign up for TrustedID to get a year's worth of free credit monitoring.

    a. In the days after the breach was announced publicly, TrustedID required that affected individuals enter a credit card number to get the service and indicated that it would automatically begin billing customers if they do not affirmatively cancel within the year.

    b. Is this "auto-billing" policy still in effect? If not, why did Equifax change the policy?
        i. Why did Equifax initially choose to use this auto-billing model for customers?
        ii. Has Equifax conducted any analyses of how many customers are expected to sign up for the service, and how many are expected to continue receiving the service after twelve months? If so, please provide the results of this analysis.
        iii. Has Equifax conducted the same analyses for a plan that does not "auto-renew"? If so, please provide the results of this analysis.

    c. Consumers initially were required to submit sensitive information to TrustedID in order to sign up for credit monitoring. What evaluations has Equifax done of its current data security environment to ensure that the victims of this hack do not, once again, have their information stolen?

I would appreciate responses to my questions by September 29, 2017.

Sincerely,

Elizabeth Warren
Ranking Member
Senate Subcommittee for Financial Institutions
and Consumer Protection