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

November 17, 2017

Mr. Paulino do Rego Barros, Jr.
Interim Chief Executive Officer
Equifax, Inc.
1550 Peachtree Street, N.W.
Atlanta, GA 30309

Mr. Mark L. Feidler, J.D.
Non-Executive Chairman
Equifax, Inc.
1550 Peachtree Street, N.W.
Atlanta, GA 30309

Dear Messrs. Barros and Feidler:

We are continuing to investigate the Equifax data breach that resulted in the theft of personal information for nearly 145.5 million American consumers. We have additional questions for Equifax as follow-up to the testimony provided by former CEO Richard Smith when he testified before the Subcommittee on Digital Commerce and Consumer Protection on October 3, 2017.

Because Mr. Smith can no longer speak for Equifax's plans going forward and due to subsequent revelations that have come to our attention, we have additional questions about the data breach, the post-breach response, and consumer protection remediation offered by Equifax. We have questions about Equifax's October 2, 2017 disclosure that "approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of 145.5 million."[1] On October 13, 2017, over a month after the company's initial disclosure, security researchers reported a security vulnerability "caused visitors to Equifax Inc.'s website. . . to encounter malicious software" due to the website's use of a discontinued web analytic plug-in called "Fireclick."[2] The continued issues consumers face when engaging with Equifax raise more questions.

---

[1] https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821
[2] https://www.wsj.com/articles/equifaxs-latest-security-foil-a-defunct-web-service-1507937742; https://gizmodo.com/equifaxs-website-redirected-people-to-malware-thanks-to-1819474245

Our intention is to continue to get answers for the 145.5 million Americans who have had their personal information compromised. Accordingly, we request written responses and, where appropriate, responsive documents to the following no later than December 4, 2017:

1. All correspondence, including emails, notes, letters, telephonic messages, text messages and/or any other written documentation between Susan Mauldin and Richard Smith from March 1, 2017 to September 15, 2017 referring or relating to the software vulnerability identified as CVE-2017-5638.

2. All correspondence, including emails, notes, letters, telephonic messages, text messages and/or any other written documentation between David Webb and Richard Smith from March 1, 2017 to September 15, 2017 referring or relating to the software vulnerability identified as CVE-2017-5638.

3. All correspondence, including emails, notes, letters, telephonic messages, text messages and/or any other written documentation between David Webb and Susan Mauldin from March 1, 2017 to September 15, 2017 referring or relating to the software vulnerability identified as CVE-2017-5638.

4. All correspondence, including emails, notes, letters, telephonic messages, text messages and/or any other written documentation between Susan Mauldin and John J. Kelley from March 1, 2017 to September 15, 2017 referring or relating to the software vulnerability identified as CVE-2017-5638.

5. All correspondence, including emails, notes, letters, telephonic messages, text messages and/or any other written documentation to or from John J. Kelley from March 1, 2017 to September 15, 2017 referring or relating to the software vulnerability identified as CVE-2017-5638.

6. All documentation prepared by Mandiant relating to the March 2017 breach and post-breach investigation presented to Equifax.

<u>Unauthorized Access to Personal Information</u>

7. Why was individual's information, including driver's license, credit card and credit dispute information, accessible via a consumer-facing dispute portal web page on Equifax.com?

8. Please describe in detail how data and information of consumers that had never submitted a dispute was accessed via the dispute portal web page on Equifax.com? What specific databases and data tables were accessed in the breach that was publicly announced on September 7, 2017?

9. Please list all other kinds of personal information that can be accessed via the dispute portal web page on Equifax.com or other consumer-facing applications/websites?

10. Were any PINs assigned to consumers necessary to lift a credit freeze compromised in the breach?

11. When Equifax announced on October 2, 2017, an additional 2.5 million U.S. consumers had partial personal information breached, the company indicated the additional population was confirmed during Mandiant's completion of the investigation process. Does Equifax anticipate any new or additional evidence of U.S. consumers affected going forward?

12. In Equifax's October 2 announcement, the company indicated "[t]o minimize confusion, Equifax will mail written notices to all of the additional potentially impacted U.S. consumers identified since the Sept. 7 announcement."

    a) Please explain the change in company protocol regarding mail notification, given the initial 143 million consumers did not receive mailed notices.

    b) Will Equifax now mail written notices to all U.S. consumers potentially affected by the breach?

13. In Equifax's October 2 announcement, the company also indicated "[t]he feature on the website that U.S. consumers may use to determine whether they may have been impacted will be updated to reflect the additional potentially impacted U.S. consumers discussed in this release by no later than October 8." On what date was the EquifaxSecurity2017.com website updated to reflect the additional population of consumers impacted?

<u>Post-Breach Response</u>

14. What steps has Equifax taken since July 29, 2017, to expedite its discovery of unauthorized access or acquisition or leaks of consumer or commercial data? What specific changes were made to the company's protocols on data security?

15. What steps has Equifax taken to notify consumers that their personal information was stolen in the breach announced on September 7, 2017? What specific changes were made to the company's protocols on data breach notification after September 7, 2017? Is Equifax directly contacting through mail, e-mail, or other means any consumers whose personal information was compromised in that breach?

16. In his testimony, Mr. Richard Smith stated "at my direction a well-known, independent expert consulting firm (in addition to and different from Mandiant) has been retained to perform a top-to-bottom assessment of the company's information security systems."

Please identify the name of the firm and provide a current point of contact with contact information for the firm.

17. According to a September 29, 2017 Bloomberg Businessweek investigation, reportedly "Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, a person familiar with the perspectives of both sides said."

    a) What warnings did Mandiant convey to Equifax management at any point in 2017, and did company officials agree or disagree with the Mandiant assessment?

    b) If Equifax disagreed with Mandiant on the security assessment, did that disagreement affect the amount of time it took to address the breach and to initiate the breach notification and offer of the TrustedID Premier services to consumers? Please explain.

    c) What impact did the disagreement have on engaging the "well-known, independent expert consulting firm" noted in Mr. Richard Smith's written testimony?

18. Did Equifax, or any third-party hired by Equifax, after two earlier data breaches in 2016 and 2017, conduct a root cause analysis and develop or obtain a set of recommendations to prevent future breaches?

    a) If so, please provide the results of any such analyses, including all issues identified and recommendations made, and identify who conducted them.

    b) Did Equifax address all of the issues identified by those analyses and implement all of the recommendations?

    c) What specific steps did Equifax take after these previous data breach incidents to improve data security?

19. According to a report on Motherboard.com on October 26, 2017, Equifax was warned by a security researcher in December 2016 that Equifax was vulnerable to attack.

    a) Did any issues or conditions identified by the third-party security researcher contribute to the breach of Equifax's Dispute Portal website?

    b) Did Equifax make any changes to the security of its servers and websites from December 1, 2016, to May 31, 2017, in response to the security warning? If so, please describe the changes made.

20. Please provide two organizational charts, one for the time period prior to the breach one current, detailing the organizational structure of the technology organization from application owner to the Chief Executive Officer.

21. Please provide two organizational charts, one for the time period prior to the breach one current, detailing the organizational structure of the security and compliance functions including the Chief Information Security Officer, Chief Legal Officer, and the Chief Executive Officer.

22. Since the breach disclosure on September 7, 2017, and the personnel changes announced on September 15, 2017:

    a) Is the Information Team (applications owners) still responsible for patching any vulnerability, and in sole possession of the asset inventory?

    b) Does the Security Team now have access to the asset inventory? If so, please describe the conditions for their access.

23. Were any of the data elements including name, social security number, address, date of birth, driver's license, credit card, or dispute information encrypted at the time of the breach announced on September 7, 2017?

    a) Did Equifax encrypt such data when transmitted? If so, how? If not, why not?

    b) Did Equifax encrypt such data when processed? If so, how? If not, why not?

24. Since the breach disclosure on September 7, 2017, under what circumstances is personal information encrypted in Equifax's system? Were any changes made to the company's protocols on encryption for consumer and commercial data after the breach? If so, please explain those changes.

25. How many individuals have signed up for the TrustedID Premier product offered by Equifax after the breach as of the date of your response to this letter?

26. Is there a back log of individuals who have indicated they would like to enroll in the product but have not yet completed the enrollment process?

    a) If there is a back log, please explain how Equifax is addressing the backlog and how long it will be before all interested individuals are enrolled in the product?

    b) If there is no back log, when where the reported issues with both the website and call centers resolved?

<u>Federal Contracts</u>

27. Equifax holds several federal contracts for data services at several key federal agencies.

    a) Was any data related to or maintained under these contracts compromised? If so, please specify which contracts were affected and which data was compromised.

    b) Did compromised data include records relating to IRS, CMS or the Social Security Administration? If so, will federal agency consumers be notified? How will they be notified?

28. Please provide the Committee with any relevant information regarding Equifax's contract to provide consumer credit verification services to the IRS, including copies of all previous contracts, all current contracts, and all protests of an award of contracts to other companies submitted by Equifax.

29. Provide a description of all contracts awarded to Equifax by the Federal Government in effect today.

Retirement Announcements

30. Please describe Richard Smith's relationship with Equifax today.

31. In a September 15th press release, Equifax indicated that the company's Chief Information Officer David Webb and Chief Security Officer Susan Mauldin were retiring with immediate effect. Were these company executives, in fact, terminated as a result of the breach?

    a) If they were not terminated, please detail their current relationship with Equifax and provide their contact information.

    b) Will the company re-evaluate and consider a clawback of all cash and non-cash compensation for all employees for which retirement announcements were made post-breach?

32. Despite the press release that personnel changes involving Mr. Webb and Ms. Mauldin were with immediate effect, there were conflicting reports of their employment relationship with Equifax.

    a) Is Ms. Mauldin still employed by the company? Is she a consultant of the company?

    b) Is Ms. Mauldin collecting any payroll or any cash or non-cash compensation?

    c) Is Mr. Webb still employed by the company? Is he a consultant of the company?

d) Is Mr. Webb collecting any payroll or any cash or non-cash compensation?

Equifax Stock Trades

33. Equifax's Chief Legal Officer, John Kelley, who is in the breach alert chain of command from the Chief Security Officer, was responsible for the approval of stock sale requests.
    a) Is this still the case?

    b) Does Equifax believe this protocol for the sale of company stock by senior executives during a data breach is appropriate?

    c) At any time since July 29, 2017, were any changes made to the company's protocols for the sale of company stock that is sold after the discovery of a security breach? If so, please detail these changes.

Credit Lock App

34. Considering the size of the breach, and the potential identity theft and fraud consumers affected face, what is the status of the new Equifax credit lock product announced on October 3, 2017?

    a) Is the rollout of the new credit lock app still on track for the end of January 2018?

    b) Are there any factors that may delay the rollout of the app? If so, please detail those factors.

    c) Will you commit to inform the Subcommittee if there are any changes in the rollout date?

35. Please describe the service that will be offered by the credit lock application and detail the steps consumers will have to take to utilize such a service.

    a) Will use of the service require consumers to consent to Equifax sharing or selling the information it collects from the service to third parties?

    b) What third parties will Equifax share or sell information collected about consumers from their use of this new credit lock tool?

36. When a credit lock is activated, what users or companies (including Equifax or its subsidiaries) can access a consumer's Equifax credit file?

37. Does freezing or locking a credit file hurt a consumer's credit score?

October 13th Incident

38. When did Equifax become aware that hackers had exploited a third-party vendor's code running on the Equifax website and was serving malicious content to visitors? How long was Equifax's website vulnerable and/or exploited?

    a) What specific website services or code did the third-party vendor provide in support of the Equifax's website? Please identify the name of the third-party vendor and provide a current point of contact for the firm including that person's contact information.

39. The Equifax website's use of a discontinued web analytic plug-in called "Fireclick" caused consumers to encounter the malicious software. Did the company's protocols on data security and breach response help identify the unauthorized intrusion? Please explain.

40. Is there any evidence of that Equifax's computer systems were accessed or any additional information about individuals' compromised? Was the consumer online dispute portal accessed or compromised?

If you have questions, please contact Melissa Froelich or Paul Jackson of the Majority staff at (202) 225-2927 and Michelle Ash or Lisa Goldman of the Minority staff at (202) 225-3641.

Sincerely,

Greg Walden
Chairman

Frank Pallone, Jr.
Ranking Member

Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

Janice D. Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection