United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

September 11, 2017

Richard F. "Rick" Smith
Chairman and Chief Executive Officer
Equifax, Inc.
1550 Peachtree Street, NW
Atlanta, GA 30309

Dear Mr. Smith,

The U.S. Senate Committee on Finance has jurisdiction over numerous federal agencies and programs that are vulnerable to fraud through the use of personally identifiable information (PII) such as names, Social Security numbers, and birth dates. The use of stolen PII results in tens of billions of dollars of fraud against the U.S. Treasury each year in the form of stolen identity, fraudulent tax refunds, Medicare and Medicaid fraud, in addition to other crimes. Furthermore, the use of stolen PII affects tens of millions of Americans each year through consumer fraud and identity theft.

On September 7, 2017, Equifax, Inc. ("Equifax") announced that, on July 29, the company discovered a cybersecurity breach in which an unknown entity or entities accessed sensitive information—including names, Social Security numbers, birth dates, addresses, in some cases driver's license numbers, and possibly other sensitive information—of approximately 143 million Americans. In addition, the breach exposed credit card numbers for about 209,000 Americans and sensitive dispute documents of approximately 182,000. Press reports indicate that the breach occurred between mid-May through July, when criminals gained access to Equifax systems and files by exploiting a vulnerability in the company's website.

Equifax, in addition to retailers, health insurers, internet companies and federal government agencies, have been targeted in security breaches in recent years which have resulted in the theft of the PII of tens of millions of Americans. The scope and scale of this breach appears to make it one of the largest on record, and the sensitivity of the information compromised may make it the most costly to taxpayers and consumers. To make matters worse, Equifax is a critical partner of the Internal Revenue Service, Centers for Medicare & Medicaid Services, the Social Security Administration and other federal agencies that are the sources and recipients of the some of the most sensitive information affecting individuals, as well as the targets of the vast majority of identity theft fraud against taxpayers.

If the names, Social Security numbers, birth dates, and other information of 143 million Americans are now in the hands of cybercriminals, this breach will cause irreparable harm to

programs within this Committee's jurisdiction by way of stolen identity refund fraud, healthcare fraud, and entitlement fraud.

To help the Committee better understand what occurred, the consequences of the breach, and how we might respond to mitigate the damage, we ask that you respond to the following question:

1. Provide the Committee a detailed timeline of the breach, including when it began, its discovery, the investigation of its scope and source, notification of authorities, efforts to notify customers and consumers, notification to the Equifax board of directors, and notification of Equifax senior executives – including, but not limited to, John Gamble Jr., Rodolfo Ploder, and Joseph Loughran.

2. Please describe Equifax's efforts to identify the scope of affected consumers and breadth of information compromised.

3. What steps has Equifax taken to identify and limit potential consumer harm associated with this breach?

4. Does Equifax plan to provide notice to each affected consumer, or will it rely on the consumer-initiated checks found at "equifaxsecurity2017.com" to inform them?

5. Your firm set up a website, "equifaxsecurity2017.com," in the wake of this announcement.

    a. The site states that "[t]he information accessed *primarily* includes names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers," (emphasis added). What other information was or may have been accessed on these accounts?

    b. As a remedy to those whose PII was accessed, Equifax is offering free, temporary access to its own identity protection services. Does the firm plan to promote its paid service to these individuals at the end of the free year?

    c. Credit monitoring can protect against identity thieves opening new accounts, but what protection does Equifax plan to offer consumers who may have had their existing credit accounts compromised?

    d. The site's terms of service contain a binding arbitration clause, binding participants of the program from participating in any class-action lawsuits that may arise from the incident. Friday morning, Equifax updated their terms of service to include an opt-out provision giving consumers 30 days to notify Equifax *in writing* that they do not wish to participate in the arbitration provision. Please explain the decision to require this opt-out to be made in writing. Do any other services provided by equifaxsecurity2017.com require consumers to contact

Equifax in writing? Are there any technical barriers preventing Equifax from providing consumers the ability to opt-out on the equifaxsecurity2017.com site?

6. Please describe the resources that Equifax has focused on its own information security. Does Equifax employ a Chief Information Security Officer? If so, to whom does this person report? How many full-time employees focus on information security? Do any members of Equifax's board of directors have a background in information security?
7. In the past 24 months, how many times has Equifax employed third-party cyber security experts to conduct penetration tests of its internal and external systems? Has the company addressed all of the issues identified by these experts and implemented all of their recommendations? Please provide us with copies of all penetration test and audit reports produced for Equifax by outside cyber security firms.

8. Does Equifax have procedures in place to receive and act on vulnerability reports from outside parties including security researchers? If so, please describe these procedures, when they were implemented, and how frequently the company acts to remediate vulnerabilities identified by third-parties.

9. Equifax has stated that the breach occurred due to criminals exploiting "a U.S. website application vulnerability...." At the time that the breach first occurred, were all of Equifax's Internet-facing applications' security updates installed? Or were these exploited due to an unknown flaw?

10. Were records related to the Internal Revenue Service, Centers for Medicare & Medicaid Service, and Social Security Administration compromised in the breach? Has Equifax alerted or will it alert its federal agency customers about the degree and scope to which federal records may have been compromised?

11. Equifax maintains *The Work Number* database, which is the largest central repository of employer-related human resources and payroll information in the U.S. The database contains millions of employee records, including those of the majority of federal government employees and 75% of Fortune 500 companies. Was this information compromised?

12. In the wake of recent IRS data losses and inadvertent disclosures, the agency directed taxpayers to send sensitive information on dependent children to Equifax – including in some cases copies of Social Security cards, birth certificates, and other information. Was this information compromised?

13. Earlier this year, identity thieves stole W-2 tax data and other employee tax records via TALX, an Equifax subsidiary that provides online payroll and tax services. Please describe this incident in detail and explain what steps Equifax took to improve cybersecurity in the wake of this intrusion.

We ask that Equifax respond electronically to this request no later than Thursday, September 28, 2017. We also ask that you provide your answers on a question-by-question basis, indicating which question you are answering. Thank you in advance for your cooperation with this request. If you have any questions, please contact [redacted]

Sincerely,

Orrin G. Hatch
Chairman, Senate Committee on Finance

Ron Wyden
Ranking Member, Committee on Finance