United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

WEBSITE: http://commerce.senate.gov

September 8, 2017

Mr. Richard Smith
Chief Executive Officer
Equifax Inc.
1550 Peachtree Street, N.W.
Atlanta, GA 30309

Dear Mr. Smith:

As the leaders of the Senate Committee on Commerce, Science, and Transportation, we are writing regarding the data security incident Equifax disclosed on September 7, 2017.

Equifax announced that the company had identified a "cybersecurity incident potentially impacting approximately 143 million U.S. consumers" and that the information accessed includes sensitive personal information such as names, Social Security numbers, birth dates, addresses, and some driver's license numbers.[1] Equifax also announced that "credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[2]

This announcement raises a number of concerns given the sensitivity of the personal data implicated and, consequently, the severity of risk consumers may face. As one of the three major credit reporting agencies in the United States, Equifax collects highly-sensitive information on American consumers. The company maintains that its investigation uncovered "no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases." Nevertheless, the nature of the information that appears to have been compromised, together with the number of potentially-impacted consumers, requires that we regard this incident as a major data security breach.

Under current federal law, the Federal Trade Commission (FTC) enforces the Safeguards Rule, which the Commission promulgated in 2002 pursuant to the Gramm-Leach-Bliley Act.[3] The Safeguards Rule applies to all financial institutions under the FTC's jurisdiction, which, according to the FTC, includes "credit reporting agencies . . . that receive information about the customers of other financial institutions." The rule requires such financial institutions to "develop, implement and maintain a comprehensive information security program" that is appropriate to the company's "size and complexity, the nature and scope of [the company's]

---

[1] Press Release, Equifax Inc., Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017).
[2] *Id.*
[3] FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. pt. 314 (2017).

activities, and the sensitivity of any customer information at issue."[4] Moreover, various state laws require breached entities to notify affected consumers in a timely manner in order to allow consumers to take steps to protect themselves from identity theft and fraud.

Protecting consumers has been and will remain a key priority of this Committee. Our goal is to understand what steps Equifax has taken to investigate what occurred, restore and maintain the integrity of its systems, and identify and mitigate potential consumer harm. Accordingly, we request answers to the following questions.

1. How many consumers does this incident affect? Please describe Equifax's efforts to identify and provide notice to these consumers.

2. With respect to this incident, what types of data does Equifax believe to have been compromised? To what extent does the data include sensitive personal information?

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

    a. Do you intend to charge fees to potentially-affected customers who wish to impose a freeze on their credit reports?

    b. For consumers who wish to avail themselves of free credit monitoring services, will you require that these consumers agree to waive certain legal rights in order to obtain such credit monitoring services?

4. What steps had Equifax taken to comply with the Safeguards Rule prior to its discovery of the incident? And what steps has the company taken subsequently to ensure compliance?

5. Please provide a detailed timeline of events, including Equifax's initial discovery of the incident, forensic investigation and subsequent security efforts, notifications to law enforcement agencies, as well as any notification to affected consumers.

In addition, please provide, when available, information regarding the source of the breach or vulnerability that gave rise to the breach, including any forensic analysis conducted.

---

[4] *Id.*

We look forward to receiving your responses as soon as possible, but by no later than 5:00 p.m. on September 25, 2017. In addition, please direct your staff to make arrangements to brief Committee staff on this matter by no later than September 15, 2017. Thank you for your prompt attention to this matter.

Sincerely,

JOHN THUNE
Chairman
Committee on Commerce,
Science, and Transportation

BILL NELSON
Ranking Member
Committee on Commerce,
Science, and Transportation