BRIAN SCHATZ
HAWAII

HART BUILDING
SUITE SH-722
WASHINGTON, DC 20510-1105
(202) 224-3934

300 ALA MOANA BOULEVARD
ROOM 7-212
HONOLULU, HI 96850
(808) 523-2061

United States Senate

September 11, 2017

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

Dear Mr. Smith:

I am writing to express serious concerns about the recent revelation that a data breach has compromised the personal information of 143 million Equifax customers. The information that was stolen, which is personal and comprehensive, could easily be used by criminals to fraudulently validate someone's identity for the purpose of opening a bank or credit account in that person's name.

The impact on Equifax's impacted customers is potentially devastating. As a result of identity theft and fraud, Equifax customers now face the risk of having debt accrued in their name. They could suffer long-lasting damage to their credit, and as a result, they could be denied loans, mortgages, employment, or even rental housing. Those approved for loans and mortgages may be charged higher interest rates. To resolve the damage done by this data breach, they will likely spend months, if not years, trying to resolve resulting errors and problems with their financial records.

As a member of the Senate Commerce Committee and Ranking Member of the Commerce Subcommittee on Communications, Technology, Innovation, and the Internet, I have several concerns about how Equifax has protected consumers' data and the steps it is taking now to protect that data. Put simply, Equifax is not doing enough.

This was not the first data breach that Equifax has suffered. For example, in May 2017, we learned that bad actors were able to access W2 tax data of employees at client companies of Equifax's payroll service subsidiary TALX, due to inadequate data security. That breach lasted almost a year, starting in April 2016.[1] In January 2017, there was data leak in which credit information of a customer at LifeLock, a credit security partner, was exposed to another user's online LifeLock portal.[2] It seems that problems with Equifax's data security go back even further than that. In April 2013 and January 2014, Equifax reported to the New Hampshire attorney general of a breach in which an "IP address operator was able to obtain . . . credit reports using sufficient personal information to meet Equifax's identity verification process."[3]

---

[1] Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, New York Times, Sept. 8, 2017, available at https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?_r=0.
[2] Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, Forbes, Sept. 8, 2017, available at https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#18199fe2677c.
[3] *Id.*

Equifax's history of data security lapses is alarming for a company whose handling of sensitive personal information for hundreds of millions of people is so core to its business.

In the wake of the breach, Equifax's response has been ineffective. The only remedy that Equifax has offered its customers has been a one-year complimentary subscription to credit monitoring, through Equifax's subsidiary, TrustedID. Equifax has not offered to pay for or reimburse credit freezes, which can cost $10 per credit reporting agency. This solution is inadequate for several reasons.

First, one year of credit monitoring is insufficient given the scope and scale of this data breach. Customers will face the risk of identity theft for years to come. In addition, credit monitoring is far from the best solution for many consumers. It can only detect identity theft and fraud after it has already occurred, while a credit security freeze can prevent identity theft and proactively protect customers' personal information.

But most importantly, it is unacceptable that Equifax is charging customers to fix Equifax's own mistakes. If even a fraction of the impacted customers implement security freezes, Equifax stands to make hundreds of millions of dollars from its security failings. Equifax should not only offer complimentary security freezes for its customers, it should also pay for or reimburse credit freezes with the other two major credit reporting agencies, Experian and TransUnion.

In light of these concerns, I ask that you please provide responses to the following questions:

1. What steps is Equifax taking to protect customers' data now that the breach has been identified? This includes Equifax's public website portal, where customers are being asked to enter the last 6-digits of their Social Security number.
2. What steps did Equifax take after previous data breach incidents to improve data security?
3. What steps has Equifax taken to ensure that TrustedID's systems do not have the same security vulnerabilities that caused this breach?
4. What efforts is Equifax making to provide support to its customers, including increasing customer support staff and dedicating resources to helping customers resolve disputes, errors, and evidence of fraud on their credit reports?
5. When customers sign up for credit monitoring services through TrustedID, will they find themselves automatically enrolled in a paid subscription product at the end of the complimentary year?

I also urge you to take the following steps to ensure that your customers receive the help they need to prevent identity theft and fraud:

1. Pay for or provide reimbursements for security freezes at each of the three major credit reporting agencies, *i.e.,* TransUnion and Experian in addition to Equifax.
2. Provide impacted customers with information about the importance of placing security freezes on credit reports in order to prevent identity theft.
3. Extend unlimited free credit monitoring services for impacted customers.
4. Undertake an independent security audit of Equifax, and its subsidiaries, to ensure the integrity of its data systems.

I would appreciate a response on these questions and follow up actions by September 29, 2017. I also look forward to a public hearing on this matter before the Senate Commerce Committee in the near future.

Thank you,

Brian Schatz
U.S. Senator