

United States Senate

September 15, 2017

Craig Boundy
Chief Executive Officer
Experian North America
475 Anton Blvd.
Costa Mesa, CA 92626

Dear Mr. Boundy:

I write regarding last week's announcement of the massive breach at Equifax that allowed criminal hackers access to sensitive personal information – including Social Security numbers, birth dates, credit card numbers, and driver's license numbers – for as many as 143 million Americans. I am deeply troubled by this attack – described as “one of the largest risks to personally sensitive information in recent years” – and I am concerned that it will hurt millions of consumers for years to come.

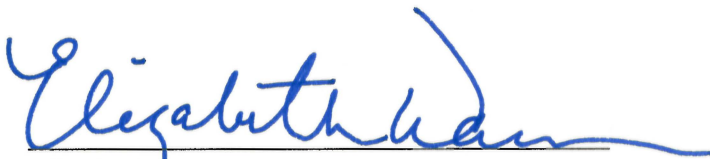
The data held by your company was not affected by the breach at Equifax. But the breach still raises two important questions about your industry as a whole. First, given the nature of data stolen, I am concerned that criminals could seek to open fraudulent lines of credit using the victims' information. It is critical that Experian coordinate with Equifax and TransUnion to reduce that risk. In addition, like Equifax, Experian holds vast amounts of sensitive, personal data about tens of millions of consumers. And like Equifax, your company has collected this data largely without consumers' knowledge or their explicit permission. Given the breach at Equifax, your company must be able to ensure consumers that their personal information is safe, and must redouble your efforts to ensure that hackers do not gain access to personal information.

To provide consumers with clarity on the danger of identity theft in the aftermath of the Equifax breach, to provide the public with information about the risk of further data breaches, and to address concerns about the credit ratings industry as a whole, I ask that you answer the following questions by September 29, 2017:

1. Did Equifax inform your company of the breach prior to the public announcement on September 7, 2017? If so, when did Equifax first inform your company about the data breach? What kind of notice did Equifax provide and how did it describe the breach to you?

2. What steps did you take after you learned of the breach to reduce the risk that hackers would use stolen data from Equifax to open fraudulent lines of credit?
3. What additional steps did you take after you learned of the breach to secure your own consumer data?
4. Do you have any evidence indicating whether there were efforts by hackers to access your data during the summer 2017 time period in which Equifax was hacked? Do you have any evidence of hackers attempting to access consumer data held by your company since the Equifax data breach was made public?
5. Have there been any data breaches at your company in the last five years? Please provide a list of all incidents, including information on the extent of the breach, how many consumers were affected, and what information was compromised.
6. Have you coordinated with Equifax and security experts to make sure that hackers cannot gain access to your data using the same techniques they used to access data at Equifax?
7. What steps do you recommend consumers take with regard to any data held by your company if they are concerned that their identities have been stolen as a result of the Equifax breach?
8. Do you have a plan in place to respond to a large-scale security breach? If so, please provide a copy of this plan.

Sincerely,



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