

September 22, 2017

The Honorable Elaine Duke
Acting Secretary
Department of Homeland Security
Washington, D.C. 20528

Jeanette Manfra
Acting Deputy Undersecretary of Cybersecurity
Department of Homeland Security
Washington, D.C. 20528

Dear Acting Secretary Duke and Acting Deputy Undersecretary Manfra:

I write regarding the recent announcement by Equifax that a massive security breach allowed hackers to access the sensitive personal information of as many as 143 million Americans.

Equifax recently confirmed that the United States Computer Emergency Readiness Team (“US-CERT”) put out a public notice months before the hack about the exact vulnerability that hackers exploited to gain access to Americans’ personal information. As you know, US-CERT is a division of the Department of Homeland Security and its mission includes “exchanging critical cybersecurity information with trusted partners ... [d]eveloping timely and actionable information for distribution to ... private industry ... [and] [r]esponding to incidents and analyzing data about emerging cyber threats.”¹

In this case, it appears that US-CERT did its part to notify Equifax and other companies of this threat, but the warning was ignored or not appropriately addressed by Equifax. When the company released additional information “as part of the company’s ongoing review of the cybersecurity incident,”² it confirmed that the “attack vector used in this incident occurred through a vulnerability in Apache Struts,” an application that supports the company’s online dispute portal.³ The release also indicated that “[t]he particular vulnerability... was identified and disclosed by U.S. CERT in early March 2017,” two months before the unauthorized access began on May 13th.⁴

¹ “About Us,” *US-CERT* (online at <https://www.us-cert.gov/about-us>).

² “Equifax Releases Details on Cybersecurity Incident, Announced Personnel Changes,” *Equifax* (Sept. 15, 2017) (online at <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>).

³ *Id.*

⁴ *Id.*

Despite the US-CERT warning, Equifax appears to have failed to address this vulnerability before the attack months later. With the personal financial data of more than one hundred million Americans at risk, Equifax was unable or unwilling to adequately address an identified security risk. While Equifax claims it “took efforts to identify and to patch any vulnerable systems in the company’s IT infrastructure,”⁵ it has not explained how the vulnerability US-CERT identified went unaddressed.

It is also unclear exactly how hackers exploited this vulnerability to gain information that puts more than 140 million Americans at risk. According to an intelligence security expert, “when you successfully exploit a web-application bug like this you will become the system user who owns the web server process.”⁶ But that system user should “have as little privilege as possible on the server itself,” at least according to best practices.⁷ Unfortunately, this means that “hackers could have found credentials or other information...right away if Equifax didn’t have proper protections in place.”⁸

I am deeply concerned about Equifax’s failure to address the vulnerability US-CERT identified. Companies like Equifax that collect massive amounts of data on millions of Americans should have the most robust data security practices. At a minimum, that means addressing clearly identified cybersecurity threats as quickly as possible.

In order to more fully understand the vulnerability in Equifax’s security, their failure to address the problem, and what can be done to prevent this from happening in the future, I respectfully request that you provide me with the following information no later than October 13, 2017:

1. Did Equifax acknowledge receiving the warning from US-CERT? Did the company follow up with US-CERT to seek additional information about the vulnerability or to obtain recommendations about how to address the vulnerability? Does US-CERT typically consult in this manner with private sector companies?
2. What efforts did Equifax take that you are aware of to address the Apache Struts vulnerability?
3. What are the duties of Equifax when notified of a vulnerability such as the one you identified to them in March 2017? What authorities does US-CERT have to ensure that private-sector entities like Equifax take appropriate action when presented with warnings of cybersecurity risks?

⁵ *Id.*


⁶ Lily Hay Newman, “Equifax Officially Has No Excuse,” *Wired* (Sept. 14, 2017) (online at <https://www.wired.com/story/equifax-breach-no-excuse/>).

⁷ *Id.*

⁸ *Id.*

4. In the last year, have you discovered or notified Equifax of any other vulnerabilities in their security? As far as you know, have they addressed these vulnerabilities?
5. In the last year, have you discovered or notified TransUnion or Experian – the two other large credit reporting agencies – of any vulnerabilities in their security? As far as you know, have they addressed these vulnerabilities?
6. I understand that the mission of US-CERT is primarily to protect civilian Federal systems. Were any Federal agencies affected by the Apache Struts vulnerability? If so, what measures did you take to prevent unauthorized access to government data? Were those measures successful?

Sincerely,



Elizabeth Warren
United States Senator