

Chairman Walden - Opening Statement
“Oversight of the Equifax Data Breach: Answers for Consumers”
Digital Commerce and Consumer Protection Subcommittee
October 3, 2017

We are here today to do what it appears Equifax failed to do over the last several months: put consumers first. Our job is to get answers for the more than 145 million Americans who have had their personal information compromised and now fear that they could be victims of fraud at any time.

How could a major U.S. company like Equifax, which holds the most sensitive and personal data on Americans, so let them down? It's like the guards at Fort Knox forgot to lock the doors and failed to notice thieves emptying the vaults.

The American people deserve to know what went wrong. We want a clear timeline of events, and to understand what to expect moving forward.

As Chairman of the Energy and Commerce Committee, I've tried to put consumers at the forefront of everything we do. Today we will begin to get answers for the public, hold Equifax accountable, and make clear that businesses holding Americans' sensitive information have a responsibility under existing laws to protect those data.

Today gives whole new meaning to Mr. Smith Goes to Washington. It's not a run on the bank at issue, it's a run on the financial records of 145 million Americans. The consequence and inconveniences for our fellow citizens is every bit as important to discuss today as the reasons behind why this breach occurred in the first place.

Richard Smith, the former Chairman and CEO of Equifax at the helm during and immediately after the breach, is here to testify. Mr. Smith, we expect your candor and full cooperation as we follow the facts in this case.

While there is no such thing as perfect security, companies do have a legal obligation to protect sensitive consumer data. This diligence is necessary to both comply with existing law and, maybe more importantly, earn and keep the public's trust in our data driven economy.

Given the size of the breach and the sensitivity of the data, we expect to learn more about how Equifax failed to secure its systems and what contingency plans were in place.

Further, we need to understand how information flowed through the organization and when you and other senior executives were notified about the breach. In other words, how important was cybersecurity to you as CEO and to the rest of your executive team? Did your employees have a way to report to you if they had concerns about how the security team was functioning?

While there are still many questions that need answers, a few details have emerged. First, the vulnerability that the hackers used to get into the Equifax system was discovered in early March. From the beginning, the vulnerability was described as critical and easily exploitable. That information was pushed out through multiple security information sharing channels, including by the U.S. Computer Emergency Readiness Team, to Equifax's Chief Security Officer.

For some period of time between March and August 2017, the hackers were able to sit on Equifax's system and siphon out 145 million records without being detected. How did this go unnoticed? Further, is there a process in place to raise flags or alarms when massive amounts of data are pulled out of the Equifax system?

Then there are the questions about Equifax's response for consumers.

- Why was the consumer-facing website created on a separate domain from the main Equifax website?
- Did anyone raise concerns about creating more consumer confusion with a separate website?
- Are consumers able to sign up for the products offered by Equifax today?
- How many consumers have placed a fraud alert on their account or frozen their credit?

On top of all of the other issues, multiple times Equifax tweeted the wrong URL directing consumers to the wrong website to check if they were a part of the breach. Talk about ham-handed responses. This is unacceptable. And it makes me wonder whether there was a breach response plan in place, and if anyone was in charge of overseeing and executing that plan.

I have to agree with the interim CEO, there is "insufficient support for consumers."

It's important that as Congress does its work on public policy issues, that the Federal Trade Commission and law enforcement agencies continue with their work, especially in light of recent reports that indicated there are markers of nation-state activity.

But today, Mr. Smith, I, the rest of this committee, Congress, and the country expect answers. After all, the buck stops with you, as CEO.