Opening Statement of Chairman Bob Latta
Subcommittee on Digital Commerce and Consumer Protection
"Oversight of Equifax Data Breach: Answers for Consumers"
October 3, 2017

Good morning, today we are here to get the facts to learn what happened at Equifax that led to the personal information of over 143 million Americans being stolen. Americans deserve to know what Equifax is doing to fix the problems and help individuals that are impacted.

We must find out what happened.

The public deserves to know what happened and what steps are being taken to protect their sensitive data going forward.

Today's hearing needs to shed some much needed light on this breach. We have received assurances from Equifax that Mr. Smith can speak for the company on

concrete remediation steps the company took in the aftermath to secure its computer systems and to protect affected U.S. consumers, as well as what happened when he was the Chief Executive.

As Chairman of the Digital Commerce and Consumer Protection Subcommittee, I often speak about the fact that we live in a digitally-connected world. That fact of life can have many positive implications, far and wide-ranging, for commerce, trade, communications and entertainment.

This Equifax breach is a massive reminder of the bad actors that exist and of the security challenges confronting our digitally-integrated and data-powered economy. In this case, sensitive personal information that is used to

build credit histories and allow individuals to engage in commerce—open credit cards, buy cell phones and appliances, and secure mortgages has been compromised.

Reasonable security measures must be implemented, practiced, and continually improved by companies that collect and store data in order to guard against unauthorized access to sensitive personal information. Otherwise, consumers can face substantial financial harm. This risk is deeply concerning to me, and I know the other Members of this Subcommittee share that view.

Priority number one: We must protect Americans and work to safeguard their personal information online.

The recent Equifax data breach is unprecedented and it is also unique because of the sensitivity of information

stolen— including full nine-digit social security numbers. Over 143 million Americans are potentially impacted. This represents approximately 44% of the total U.S. population. In my home State of Ohio, approximately 5.2 million consumers are likely affected.

Based on the information released by Equifax, we are informed that the massive amounts of personal and financial information was accessed from mid-May through July 2017, including names, birthdates, addresses, and in some cases, driver's license information. In addition, over 200,000 people had their credit card information stolen, and over 180,000 people had credit dispute documentation stolen.

That is a staggering amount of sensitive personal information. It impacts an extraordinary number of credit-visible Americans, that in the hands of bad actors that could result in fraud or identity theft. We need these numbers confirmed.

Today, we must understand the following:

First, how did the hackers get into Equifax's system for so many weeks and pull so much information out of the system without being detected?

Second, what processes and procedures were in place in the event of such a breach and were those processes followed? There are many questions as to who knew what, and when this information was known? This will have implications in other ongoing investigations.

Further, the Chief Information Officer and Chief Security Officer made retirement announcements shortly after the public notice of the breach and have not been available for questions about their role.

And, despite months of delay, why was Equifax's notification and consumer protection process still met with misinformation, glitches, and overall confusion? For example, there were numerous reports of difficulties accessing Equifax's dedicated website or call centers. And there were dismaying reports that the official Equifax Twitter account directed consumers to a fake website.

I think the American public deserves to know the facts about when and how Mr. Smith, company management, and the board of directors were made aware

its systems were vulnerable to hackers and over 143 million sensitive personal data records were stolen. Then, what were the steps taken and in what timeframe to notify and help individuals that were impacted.

I look forward to getting answers to these and many more questions for the American public this morning.