Opening Statement of Chairman Bob Latta
Subcommittee on Digital Commerce and Consumer Protection
"Securing Consumers' Credit Data in the Digital Age"
November 1, 2017

One month ago, this Subcommittee was the first to hear testimony from former Equifax CEO Richard Smith about how his company's failure to protect against a known data security vulnerability led to the loss of over 145 million Americans' sensitive information.

Our investigation continues into the Equifax breach and today's hearing is another step to get answers for the public about:

- what the industry response has been to this breach,
- if the cybersecurity landscape has shifted as a result of the breach, and
- what laws and regulations are at issue.

On Friday, our Full Committee Chairman Greg Walden authored an op-ed in which he raised questions about how actions taken by businesses built around individual's data affect security,

privacy, and individual's online identities. All of these issues are critically important to understand in our digital economy and I look forward to working with the Chairman and my fellow subcommittee chairman on these issues in the coming months.

The Equifax data breach was a stark demonstration of the responsibility that credit bureaus and all companies have when holding millions of Americans' sensitive information. In fact, Congress has recognized the sensitivity of this data and specifically enacted laws regarding the credit bureau business model.

Today, we are looking for answers about how best to secure consumers' credit data in order to protect against another breach of this magnitude.

We want to shine a light on security practices and understand the path forward to restore confidence to U.S. consumers.

Credit bureaus prepare credit reports based upon individuals' financial transactions history to provide such reports to third parties.

For example, lenders, including banks and retailers, use credit reports and related data to evaluate the likelihood that borrowers will repay their loans.

This credit information assists consumers in accessing credit, buying a house, or securing a job.

However, consumers may not know or understand what data has been collected on them and how it's being used by the credit reporting industry and their paying customers, including the Federal government.

The subcommittee has taken a comprehensive review of the circumstances around the breach.

For example, it came to our attention last month that the Internal Revenue Service had awarded a no-bid contract to Equifax.

On October 10th, Ranking Member Schakowsky and I, along with Chairman Walden and Ranking Member Pallone, sent a bipartisan letter to IRS Commissioner John Koskinen raising concerns about the IRS's decision to award a contract to Equifax for identity verification services in the aftermath of the Equifax breach. The contract has since been rescinded.

We also sent a bipartisan letter on October 16th to the General Services Administration about the agency's consideration of data security practices when vetting vendors like Equifax and awarding government contracts. We look forward to GSA's response.

-I thank my colleagues across the aisle for working together on this serious matter. Chairman Walden and I remain committed to working in a bipartisan fashion to get answers for the American public and to hold Equifax accountable.

When former CEO Richard Smith came to Washington last month, he said quote: "the breach occurred because of both human error and technology failures."

These quote-unquote “errors” and “failures” allowed criminals to access over 145 million Americans’ data.

As a result, names, addresses, birthdates, and full nine-digit Social Security numbers were exposed.

And certain driver’s license, credit card, and credit dispute information were taken.

If your credit card information is stolen, you can contact Visa or MasterCard and they’ll reissue you a new card and credit card number.

If your Social Security number is stolen, it’s much, much more complicated to get a new number.

A Social Security number is intrinsically tied to each and every one of us.

According to the FTC, there were nearly 400,000 identity theft complaints in 2016, or 13 percent of all consumer complaints received, with 29 percent of consumers reporting that their data was used to commit tax fraud in 2016.

Consumers also reported that their stolen data was used for credit card fraud; rising to more than 32 percent in 2016 from nearly 16 percent in 2015.

In the aftermath of the Equifax breach, months later, consumers may still be confused about how best to protect themselves.

All of this is disconcerting, and frankly unacceptable.

This Subcommittee, and agencies like the Federal Trade Commission, have been providing useful information to consumers in the aftermath of the Equifax breach.

But the post-breach consumer protection responses from Equifax have yet to be reassuring.

Data collected and stored by credit bureaus must be protected and safeguarded at all times, and when a breach happens consumers need swift and concrete answers from the company affected.

Our Subcommittee members continue to ask whether consumers can be confident in the security of their data.

There are important questions about the best ways to protect sensitive data, including cybersecurity standards, trends, best practices and emerging threats particularly with respect to known cybersecurity vulnerabilities.

There are also important questions about the regulatory landscape in which the credit bureaus operated before this massive breach.

For example, what is the legal and regulatory framework for credit bureaus, including the safeguards framework in the Gramm-Leach-Bliley Act and consumer protections contained in the Fair Credit Reporting Act?

Finally, what is the relationship between data breaches and incidence of identity theft and fraud?

Data breaches may have become so commonplace that data security experts have expressed concerns about "breach fatigue."

Though there may be fatigue, Congress cannot afford to be lax or idle in its oversight over these critical issues.

I look forward to the testimony of the panel.