Opening Statement of Senator Tom Carper
"Examining Private Sector Data Breaches"
March 7, 2019

Thank you, Mr. Chairman.

According to a 2017 study by the Pew Research Center, the vast majority of Americans have personally experienced a major data breach. And about half of the country believes their personal information is less secure than it was five years ago.

Our Subcommittee initiated an investigation into the causes of private sector data breaches shortly after Equifax announced its breach in the fall of 2017. As we conducted our work, a seemingly endless stream of new, high-profile incidents were announced. One after the other, well-known companies, including Google, Facebook, Ticketfly, T-Mobile, Orbitz, Saks Fifth Avenue, Lord & Taylor, Under Armour, and, eventually, Marriott, announced that they too had suffered breaches.

Mr. Begor and Mr. Sorenson, thank you for your appearance today and for your help in better understanding how these private sector data breaches occur and what can be done to prevent them, including steps Congress can take. While my colleagues and I will have some tough questions for you, our goal here is to ensure that the mistakes and oversights that contributed to the attacks your companies suffered are well understood so that other American businesses are less likely to fall victim to hackers.

When hackers are able to obtain someone's personal information, the consequences are real. The 2017 Pew study I referenced found that more than 40 percent of the individuals polled had discovered fraudulent charges on their credit cards. Others reported that someone had attempted to take out loans in their name, file tax returns in their name, or steal their identity.

Even when a breach victim is fortunate enough to avoid becoming a victim of crimes like these, they often deal with months or even years of hassle and worry as they swap out compromised credit and debit cards, change their online passwords, and monitor their bank accounts and credit reports for suspicious activity.

Given the vast amount of information collected on consumers these days, and the skill and relentlessness of the hackers seeking to steal that information, it is critical that businesses make cybersecurity a priority. The constant stream of data breach notifications we see year in and year out is a sign to me that we could, and should, be doing a lot better.

That is certainly the case with Equifax.

Equifax and its two main competitors –TransUnion and Experian – have built their business models around the collection and dissemination of consumers' most sensitive financial information. This includes names, nicknames, dates of birth, Social Security numbers, telephone numbers, current and former addresses, account balances, and payment histories.

This data collection is not something consumers can opt out of. Credit reporting agencies collect personal information without our knowledge or explicit authorization.

If someone shops regularly at a retail chain that gets hacked, that person can opt not to shop there any longer if doing so makes them uncomfortable. They cannot, however, keep their information away from Equifax.

Knowing this, you would think that protecting the sensitive information its entire business relies on would be Equifax's top priority. Yet information obtained by the Subcommittee and included in a bipartisan report released last night illustrates a years-long neglect of basic cybersecurity practices and a decision by company officials to prioritize the ease of doing business over security.

In 2015, Equifax officials learned through an internal audit that the company's IT systems were riddled with thousands of unpatched vulnerabilities, hundreds of them deemed critical or high risks. They also learned that the company lacked a mature inventory of its IT assets, making it more difficult to address problems as they arose.

By the time the Department of Homeland Security announced, in March 2017, that versions of the widely-used web application software Apache Struts included a serious security flaw, Equifax had still not properly responded to its 2015 audit findings or brought its cybersecurity practices in line with industry standards.

Despite being informed that the announced flaw in Apache Struts was extremely dangerous and easy to exploit, Equifax officials appear to have approached the challenge it presented with no sense of urgency whatsoever.

Scans of the company's network failed to find the vulnerable version of Apache Struts it was using, and key staff who were in positions to make the necessary security enhancements were left off of internal communications. The vulnerability was discussed at regular security meetings held in March and April of 2017, but it's not clear who attended those meetings. Senior managers interviewed by the Subcommittee, who were nominally in charge of IT management and cybersecurity at Equifax, told Subcommittee staff that they did not regularly attend the meetings themselves.

Former top Equifax officials we interviewed were very frank about the priority they placed on cybersecurity. One key former security official told Subcommittee staff that "security wasn't first" at Equifax. The company's former Chief Information Officer was extremely dismissive of the importance of key security processes during his interview, saying that he considered the patching of security flaws to be a "lower level responsibility that was six levels down" from him.

There's no evidence that these two individuals or any other top executives at Equifax directed staff to take steps to update the company's IT asset inventory or conduct a more thorough search for the vulnerable Apache Struts software.

This lack of initiative would be bad enough on its own, but Equifax also left itself blind to incoming attacks by allowing the tools it needed to monitor for malicious web traffic to expire. So when hackers moved in May 2017 to attack Equifax through a version of Apache Struts still

in use on the company's web site, nobody saw them coming. What's more, nobody discovered them until July – 78 days after the hackers first gained entry.

During the 78 days the hackers spent inside of Equifax's IT network, they accessed multiple data repositories containing information on more than 145 million people.

There are tools available that could have sent alerts to Equifax staff as the hackers manipulated the information in the databases, but Equifax had not installed them.

Once Equifax found the hackers at the end of July 2017, Equifax executives waited an additional six weeks before letting the public know what had happened.

So, because Equifax was unaware of all the assets it owned, unable to patch the Apache Struts vulnerability, and unable to detect attacks on key portions of its network, consumers were left unaware for months that criminals had obtained their most sensitive personal and financial information. Consumers were also unaware that they should take steps to protect themselves from fraud.

And importantly, these failures stand in stark contrast to the experiences of TransUnion and Experian, which both quickly identified and addressed the same Apache Struts vulnerability, and have not announced data breaches.

The data breach announced by Marriott this past November doesn't appear to have been caused by the kind of cultural indifference to cybersecurity the record indicates existed at Equifax. Rather, it looks like Marriott inherited this attack through its acquisition of Starwood. But the size of this breach – up to 500 million people were reported to have been affected at one point – requires that we take a close look and learn what happened and why.

I have questions about Marriott's data retention policies. For example, I understand why a hotel chain might collect passport information in some cases, but I don't know why it would need to maintain records of millions of guest passport numbers as appears to have occurred in this case.

This incident also raises questions about the degree to which cybersecurity concerns do and should play a role in merger and acquisition decisions. In Starwood, Marriott acquired a company that it knew had serious cybersecurity challenges and had actually been attacked before. Despite this, Marriott chose to initially leave Starwood's security system in place after acquiring the company. We need to learn more about the priority Marriott executives chose to place on addressing security flaws at Starwood as it worked to integrate its systems into its own.

What we do know today is that large-scale data breaches are not going to stop. We can't afford to shrug our shoulders and write them off as a cost of doing business. There are real costs to approaching cybersecurity challenges with this frame of mind, and real harm that can occur both to consumers' pocketbooks and companies' bottom line.

Here in Congress, I think it's long past time for us to come to agreement on a federal data security law that lays out for private industry what we expect from them, both in data protection and data breach notification.

We also need to ensure that the system we've established for sharing information on cyber threats and cybersecurity best practices is as effective as it could be. If a company as large and sophisticated as Equifax can fail so badly at implementing basic cybersecurity practices, we can certainly do a better job making clear what will and won't work when it comes to blocking hackers and preventing data breaches.

My thanks again, Mr. Chairman, for the work you and your staff put in with us on this complex and important issue. I look forward to hearing from our witnesses.