EXAMINING PRIVATE SECTOR DATA BREACHES
CHAIRMAN ROB PORTMAN
OPENING STATEMENT

March 7, 2019

This hearing of the Permanent Subcommittee on Investigations will come to order. [gavel]

It seems no industry is immune from data breaches that expose sensitive consumer information.

- Some of the biggest recent breaches have included Google+, Uber, Facebook, and the department store Saks Fifth Avenue.

- Government agencies have also suffered breaches, including over 20 million security clearance background files held by the Office of Personnel Management.

Locating network vulnerabilities that hackers can exploit to gain access to sensitive information is an issue that Senator Hassan and I have worked on together from the full committee.

Earlier this year, the President signed our Hack DHS Act, which will strengthen DHS's cybersecurity, by using "white-hat" hackers to locate previously unknown vulnerabilities in DHS networks.

Last night, Sen. Carper and I released a report on how the Equifax data breach occurred and how hackers were able to steal personal and financial data on over 145 million Americans.

That report documents how Equifax failed to follow basic cyber security practices, which prevented the company from identifying and patching an exploitable vulnerability on its system.

During the course of our investigation, we also learned the company failed to preserve important documents related to the breach.

- Equifax employees told us they frequently used a chat application called Microsoft Lync.

- When Equifax first discovered the breach on **July 29**, the Security team used the chat platform to discuss the hacked system and even the company's response.

- Equifax issued a notice not to destroy documents related to the breach on **August 22, 2017**, but failed to set the chat platform to archive any of these chats until **September 15, 2017, a month-and-a-half after** the breach was discovered on July 29.

- Prior to **September 15**, Equifax was not archiving any Lync chats based on its document retention policy. Counsel for Equifax told the Subcommittee they could not find any of the chats Equifax employees told us about documenting the discovery of the breach.

- As such, the Subcommittee is left with an incomplete record.

After discovering the breach, Equifax **waited six weeks** to disclose on September 7, 2017 that hackers had compromised its collection of personal and financial information on over 145 million Americans.

Adding to this delay, the hackers had access to the information since May 13, 2017, **three months** before they were discovered.

Equifax Chief Executive Officer Mark Begor is here to today to discuss our report's findings.

We are also going to hear today from Arne Sorenson, Marriott's Chief Executive Officer on the data breach his company disclosed in November 2018.

That breach of the Starwood reservation database occurred in July 2014, two years before Marriott acquired Starwood in September 2016.

This was not the first time Starwood suffered a data breach.

In November 2015, Starwood announced that it had discovered malware on some of its systems at hotels designed to steal credit card information at the point of sale. At the time, Starwood stated this breach did not impact its guest reservation database.

In November of 2018, Marriott announced it had discovered that a hacker had accessed the Starwood guest reservation database.

Marriott's investigation determined that the hacker had access to guest information related to 383 million guest records since 2014.

- As part of the database, the hackers also gained access to over 23 million passport numbers and 9.1 million credit card numbers, most of which were expired.

- Marriott learned of the breach on September 8, 2018, but waited almost 12 weeks to notify the public on November 30, 2018.

The goal of today's hearing and the Subcommittee's report is to fully understand these breaches; but also to find solutions.

- Companies and government agencies, alike, must take steps to protect the data consumers entrust to them.

- And when that data is compromised, we deserve to know as soon as possible so we can do everything we can to ensure criminals are not taking advantage of us.

- I look forward to working with my Ranking Member, Senator Carper, on legislation to ensure both the protection of consumer data and prompt notification when data is compromised.

- I also want to thank Sen. Carper for his dedication to these issues, and his staff for leading this investigation.

With that, I turned to Sen. Carper for his opening statement.