

EXAMINING PRIVATE SECTOR DATA BREACHES

HEARING

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON

HOMELAND SECURITY AND

GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 7, 2019

Available via the World Wide Web: <http://www.govinfo.gov>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



EXAMINING PRIVATE SECTOR DATA BREACHES

HEARING

BEFORE THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON

HOMELAND SECURITY AND

GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 7, 2019

Available via the World Wide Web: <http://www.govinfo.gov>

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

36–304 PDF

WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio	GARY C. PETERS, Michigan
RAND PAUL, Kentucky	THOMAS R. CARPER, Delaware
JAMES LANKFORD, Oklahoma	MAGGIE HASSAN, New Hampshire
MITT ROMNEY, Utah	KAMALA D. HARRIS, California
RICK SCOTT, Florida	KYRSTEN SINEMA, Arizona
MICHAEL B. ENZI, Wyoming	JACKY ROSEN, Nevada
JOSH HAWLEY, Missouri	

GABRIELLE D'ADAMO SINGER, *Staff Director*
DAVID M. WEINBERG, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS SPINO, *Hearing Clerk*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

ROB PORTMAN, Ohio *Chairman*

RAND PAUL, Kentucky	THOMAS R. CARPER, Delaware
JAMES LANKFORD, Oklahoma	MAGGIE HASSAN, New Hampshire
MITT ROMNEY, Utah	KAMALA D. HARRIS, California
JOSH HAWLEY, Missouri	JACKY ROSEN, Nevada

ANDREW DOCKHAM, *Staff Director and Chief Counsel*
JOHN KILVINGTON, *Minority Staff Director*
KATE KIELCESKI, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Portman	1
Senator Carper	3
Senator Hassan	12
Senator Rosen	17
Senator Hawley	20
Senator Harris	22
Senator Peters	25
Prepared statements:	
Senator Portman	47
Senator Carper	50

WITNESSES

THURSDAY, MARCH 7, 2019

Mark Begor, Chief Executive Officer, Equifax Inc.; Accompanied by Jamil Farshchi, Chief Information Security Officer	7
Arne Sorenson, President and Chief Executive Officer, Marriott International	8
Andrew Smith, Director, Bureau of Consumer Protection, U.S. Federal Trade Commission	35
Puente Cackley, Director, Financial Markets and Community Investment, U.S. Government Accountability Office	37
John Gilligan, Chief Executive Officer, Center for Internet Security	38

ALPHABETICAL LIST OF WITNESSES

Begor, Mark:	
Testimony	7
Prepared statement	54
Cackley, Puente:	
Testimony	37
Prepared statement	79
Gilligan, John:	
Testimony	38
Prepared statement	90
Smith, Andrew:	
Testimony	35
Prepared statement	69
Sorenson, Arne:	
Testimony	8
Prepared statement	59

APPENDIX

Equifax Audit	98
Letter From Our President	106
February 18, 2019 New York Times Article	108
March 6, 2019 Wall Street Journal Article	112
Responses to post-hearing questions for the Record:	
Mr. Begor and Mr. Farshchi	116
Mr. Sorenson	121

EXAMINING PRIVATE SECTOR DATA BREACHES

THURSDAY, MARCH 7, 2019

U.S. SENATE, PERMANENT SUBCOMMITTEE ON
INVESTIGATIONS,
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL
AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:05 a.m., in room SD-106, Dirksen Senate Office Building, Hon. Rob Portman, Chairman of the Subcommittee, presiding.

Present: Senators Portman, Hawley, Johnson, Carper, Hassan, Harris, Rosen, and Peters.

OPENING STATEMENT OF SENATOR PORTMAN¹

Senator PORTMAN. This hearing of the Permanent Subcommittee on Investigations (PSI) will come to order.

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

Some of the biggest breaches have seen recently include Google, Uber, Facebook, and the department store Saks Fifth Avenue.

Government agencies have not been immune from this. They have also suffered significant breaches, including over 20 million security clearance background files that were held by the Office of Personnel Management (OPM).

Locating network vulnerabilities that hackers can exploit to gain access to sensitive information is a key issue. Actually, Senator Hassan and I have worked on together with some specific legislation. She is here this morning.

Earlier this year, the President signed our Hack DHS Act, as an example, into law, which will strengthen DHS' cybersecurity by using "white hat" hackers to locate previously unknown vulnerabilities in the Department's systems.

Last night, Senator 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 cybersecurity practices and protocols, 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.

¹The prepared statement of Senator Portman appears in the Appendix on page 47.

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

When Equifax first discovered the breach on July 29, 2017, the security team used that chat platform to discuss the hacked system and even the company’s response.

Our report uncovered that Equifax did not issue a notice not to destroy documents related to the breach until August 22, 2017, and 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, again, back on July 29th.

Prior to September 15, Equifax was not archiving any Lync chats based on its own 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 a result, the Subcommittee is left with an incomplete record. So are the American people.

After discovering the breach, Equifax waited 6 weeks to disclose to the public on September 7, 2017, that hackers had compromised its collection of personal and financial information, again, on over 145 million Americans.

Adding to this delay, the hackers had access to the information since May 13, 2017, 3 months before they were discovered.

Equifax Chief Executive Officer (CEO) Mark Begor is here today to discuss our report’s findings.

We are also going to hear today from Arne Sorenson, Marriott’s CEO, on the data breach his company disclosed in November 2018. That breach of the Starwood reservation database occurred in July 2014, 2 years before Marriott acquired Starwood in September 2016.

But this was not the first time Starwood suffered a databreach.

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 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 that 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 focus on the future, to focus on solutions.

Companies and government agencies alike must take steps to protect the data consumers entrust to them. That is clear.

When that data is compromised, we need to know as soon as possible so we can do everything we can to ensure criminals are no longer taking advantage of us as consumers. That seems clear.

I look forward to working with my Ranking Member, Senator Carper, and others on this Committee, including the Chairman and Senator Hassan, and ensuring that we can move forward with leg-

isolation that ensures both the protection of consumer data and prompt notification when data is compromised.

I also want to thank Senator Carper and his staff for their dedication to these issues and him and his staff for leading this investigation.

With that, I turn to Senator Carper for his opening statement.

OPENING STATEMENT OF SENATOR CARPER¹

Senator CARPER. Thanks. Thanks, Mr. Chairman. Our thanks to both of our witnesses this morning for joining us.

I want to take a moment to say a special thanks to members of the minority staff and the members of the majority staff who have worked hard for months to prepare us for this day.

According to a 2017 study by the Pew Research Center, the vast majority of Americans have personally experienced a major databreach. My guess is most of us in this room on this side of the panel are among them. About half of our country believes their personal information is less secure than it was 5 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, we 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 that we can take. While my colleagues and I will have some tough questions for you, as the Chairman has indicated, 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 referred to 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. Several of those things have happened to my own family and I suspect to the families of many of us in this room.

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 activities.

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 at the very top level of a company—the

¹The prepared statement of Senator Carper appears in the Appendix on page 50.

board and the CEOs, as well. 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.

As my colleagues have heard me say many times, everything I do I know I can do better. The same is true of all of us. In this one particular area, we need as a country to do a whole lot better. It is a shared responsibility.

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. That 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 our 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 this 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 information technology (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 networks 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 internal communications. The vulnerability was discussed at regular security meetings held in March and April 2017, but it is not clear who attended those meetings. Senior managers interviewed by the Subcommittee were nominally in charge of IT management and cybersecurity at Equifax, and they 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 was not first” at Equifax. That is an understatement. The company’s former chief

information officer (CIO) 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 is 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. When hackers moved in May 2017 to attack Equifax through a version of Apache Struts still in use on the company’s websites, nobody saw them coming. What is 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, and probably half the people in this room are among them.

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 6 weeks before letting the public know what had happened—6 weeks.

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.

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.

I have a friend, and when you ask him how he is doing, he says, “Compared to what?” I think the obvious question here is for Equifax compared to TransUnion and Experian.

The data breach announced by Marriott this past November does not 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 do not 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 that 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 cannot 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 to the companies' bottom lines.

Here in Congress, I think it is 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 in data breach notification.

We also need to ensure that the system we have established for sharing information on cyber threats and cybersecurity best practices is as effective as it can be and it is updated over time. 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 will not work when it comes to blocking hackers and preventing data breaches.

My thanks again, Mr. Chairman, for the work that you and your staff and my staff have put in on this complex and important issue. We look forward to hearing from our witnesses today. Again, thank you for joining us.

Senator PORTMAN. Thank you, Senator Carper.

I would now like to call the first panel of witnesses. First we have Mark Begor, who is the chief executive officer of Equifax. He has served in that capacity since April 2018. Again, as we just heard, the Equifax breach was discovered in July 2017.

Second, Arne Sorenson is here. He is the president and chief executive officer of Marriott International, Inc. He has held that position since 2012. Again, as we just heard, Marriott acquired Starwood in 2016. The breach occurred at Starwood in 2014 and was discovered in 2018.

We are also going to swear in someone else this morning, Jamil Farshchi, who is the current chief information security officer (CISO) at Equifax. It was requested should Mr. Begor need some special expertise, technical assistance, so I am going to ask you to raise your hand as well.

It is the custom of this Subcommittee to swear in all of our witnesses, so at this time I would ask you all to please stand and raise your right hand. Do you swear the testimony you will give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. BEGOR. I do.

Mr. FARSHCHI. I do.

Mr. SORENSON. I do.

Senator PORTMAN. Let the record reflect the witnesses, all three, answered in the affirmative.

Gentlemen, all your written testimony will be printed in the record in its entirety, so I would ask that you try to limit your oral testimony to 5 minutes.

Mr. Begor, we will hear from you first.

**TESTIMONY OF MARK BEGOR,¹ CHIEF EXECUTIVE OFFICER,
EQUIFAX INC.; ACCOMPANIED BY JAMIL FARSHCHI, CHIEF
INFORMATION SECURITY OFFICER, EQUIFAX INC.**

Mr. BEGOR. Chairman Portman, Ranking Member Carper, and distinguished Members of the Subcommittee, thank you for the opportunity to be here today. I am Mark Begor, Chief Executive Officer of Equifax. With me today is Jamil Farshchi, our Chief Information Security Officer.

Let me begin by expressing my personal regret for the disruption that our 2017 cyber attack had on millions of Americans.

Cyber crime is one of the greatest threats facing our country today. U.S. corporations are continually fighting criminals that operate outside the rule of law and attempt to steal data for their own gain. These attacks are no longer a hacker in the basement attempting to penetrate a company's security perimeter, but instead are carried out by increasingly sophisticated criminal rings and, even more challenging, nation-states that are well funded or the military arms of nation-states. These attacks on U.S. businesses are attacks on U.S. consumers and are attacks on America. This war is getting more challenging and more sophisticated, and there is no end in sight. Fighting these attackers will require cooperation between government, law enforcement, and the private sector.

We appreciate that Members of this Subcommittee have introduced legislation that promotes this type of partnership, and we support these efforts.

The fact that Equifax suffered a data breach does not mean the company did not have an appropriate data security program or that the company failed to take cybersecurity seriously. I understand that before the attack, the company's security program was well funded and staffed and leveraged strong administrative and technical safeguards.

In April 2018, when I joined Equifax, I made a personal commitment internally and externally to build a culture within Equifax where security is a part of our Deoxyribonucleic acid (DNA) and committed that Equifax would be an industry leader around data security. I am proud of the leadership, cultural enhancements, and investments that Equifax has made over the past 18 months. We have added experienced senior leaders and board members to enhance our security and technology skill sets. In 2018 alone, we added close to 1,000 incremental security and IT professionals to our team. Between 2018 and 2020, we are increasing our technology and security spending by 50 percent, totaling an incremental \$1.25 billion.

We recognize that being an industry leader means actively sharing our security learnings and best practices. We have been openly sharing all of our cyber learnings with our customers, our competitors, the U.S. Government, and the rest of the private sector.

Last year, we established a number of meaningful security partnerships that will help raise the entire security community by leveraging our joint learnings.

¹ The prepared statement of Mr. Begor appears in the Appendix on page 54.

In addition to the goal of being a leader in data security, Equifax has been working diligently to support U.S. consumers. When Equifax announced the cyber attack, its response was guided by a desire to focus on helping and supporting consumers first.

Since the 2017 incident, Equifax has invested more than \$80 million to assist impacted consumers. When we announced the incident, we offered an identity theft and credit monitoring service free for all Americans, regardless if they were impacted by the cyber incident. Last November, when that service was nearing its end, Equifax voluntarily extended that protection for another year.

Going forward, we are investing over \$50 million to make it easier for consumers to interact with us, both over the Internet and in our call centers. We want to make sure we are a consumer-friendly credit bureau at every step of the way.

To close, I would like to thank Chairman Portman for holding this hearing. Equifax is committed to our mission to become an industry leader in data security, and we are investing unprecedented resources in technology, security, and people.

Thank you again for the opportunity to testify and for your focus on protecting American businesses and consumers from cyber attacks.

Senator PORTMAN. Thank you, Mr. Begor.

Mr. Sorenson, we will now hear from you.

**TESTIMONY OF ARNE SORENSON,¹ PRESIDENT AND CHIEF
EXECUTIVE OFFICER, MARRIOTT INTERNATIONAL**

Mr. SORENSON. Chairman Portman, Ranking Member Carper, and members of the Subcommittee, thank you for the opportunity to testify today.

The subject the Subcommittee is tackling—private sector cyber attacks—is an increasingly urgent one, one that has hit Marriott directly with the data security incident we announced on November 30, 2018. We deeply regret this incident and are committed to determining how it occurred, supporting our affected guests, and enhancing security measures to protect against future attacks.

For 91 years, Marriott has been in the business of serving people. We began as a small family business in Washington, D.C., serving hamburgers and root beer at The Hot Shoppes. Today we are a global hospitality company, conducting operations in all 50 of the United States and 130 countries and territories. Throughout that time, we have built our reputation by putting people first and focusing on the care of our guests.

As a company that prides itself on taking care of people, we recognize the gravity of this criminal attack on the Starwood Guest Reservation Database and our responsibility for protecting data concerning our guests. To all of our guests, I sincerely apologize. We are working hard every day to rebuild your confidence in us.

Because this incident involved the Starwood database, let me provide some background on the merger of Marriott with Starwood.

Marriott signed a merger agreement with Starwood in November 2015 and closed the transaction in September 2016. Between these two events, we obtained information about Starwood's network and

¹ The prepared statement of Mr. Sorenson appears in the Appendix on page 59.

conducting an assessment on integrating the two systems, although this inquiry was legally and practically limited by the fact that, until the merger closed, Starwood remained a direct competitor.

We made the decision to retain Marriott's reservation system as the central system for the combined group of hotels and to retire Starwood's system. Migrating all of Starwood's 1,270 hotels onto Marriott's reservation system while avoiding disruption of the reservation process was a significant undertaking that took us about 2 years. We made additional investments to enhance security of the system while it was operating.

Following the discovery of the incident, we accelerated the retirement of Starwood's reservation system and, as of December 18, 2018, are no longer using the Starwood Guest Reservation database to conduct business or operations.

Until our investigation of the incident announced on November 30, we were unaware that the Starwood Guest Reservation database had been infiltrated by an attacker. Our investigation was initiated following an alert on September 7, 2018, from a cybersecurity tool. In response, our IT team swiftly implemented containment measures. We retained industry experts to conduct a forensic investigation and deploy additional defenses.

Unraveling the scope of the attack required extensive forensic work by experts. We also contacted the Federal Bureau of Investigation (FBI), which continues its investigation. As our investigation unfolded, we learned that the intruder had been in the Starwood system since 2014.

On November 19, 2018, we determined that the intruder had accessed files containing personal information of guests who had made reservations at Starwood properties. We believe that the upper limit for the total number of guest records involved in this incident is approximately 383 million.

What do we mean by "guest records"? Take my name for an example, which is in the database multiple times with variations such as Arne Sorenson, Arne M. Sorenson, Arne Morris Sorenson, sometimes with my home address, other times with my business address, and yet again without any address. Each entry represents a separate record even though they all related to one person. We cannot confidently determine whether records with similar names, or even identical names, represent one person or multiple people, but we know that the information for fewer than 383 million unique people was involved.

In the days immediately after November 19, we worked quickly to make sure that we could share useful information with our guests. On November 30, we provided broad public notice of the incident via a press release and notification banners across Marriott and Starwood websites and apps. We stood up a website with consumer information in multiple languages as well as call centers to answer questions and offered guests free web monitoring service, among other steps.

In assessing the impact of this event, you should know that Starwood did not keep guests' Social Security numbers, and the overwhelming majority of payment card information was encrypted. To date, we have not found data removed from the Starwood database on the Internet or Dark Web, which we continue to monitor.

Finally, we know this is a race that has no finish line. Cyber attacks are a pervasive threat. We are committed to responding to these evolving threats with a layered defense approach and continuous improvement. Our founder, J. Willard Marriott, was fond of saying that success is never final. We are applying that critical review process to learn from this incident as we work diligently to regain the level of trust that our guests have come to expect from us over the years.

Thank you, and I welcome your questions.

Senator PORTMAN. I would like to thank both the witnesses for their statements, and I think they make a good point that this is a matter that requires cooperation between government and the private sector at every level.

I am going to delay my questioning until we have a chance to be sure that our two colleagues, who I know have other commitments, have a chance to ask theirs. For this first round—I will be coming back and asking some questions. I want to give them a chance first before they have to leave, and I now turn to my Ranking Member, Senator Carper.

Senator CARPER. Senator Hassan, if you and Senator Rosen have other obligations, go ahead and ask your questions.

Senator HASSAN. I am fine if you want to go ahead.

Senator CARPER. All right. Thanks.

Again, thank you. I think it was Maya Angelou who used to say, “People may not remember what you say, they may not remember what you do, but they will remember how you made them feel”—Maya Angelou. “People may not remember what you say, they may not remember what you do, but they will remember how you made them feel.” First, I want to say I was glad to hear both of you apologize. As I used to say to my kids, who are now grown, “The three most important words are ‘please’ and ‘thank you.’ The couple others that mean a lot are ‘I am sorry,’ especially when we screw up.” Especially with respect to Equifax, the amount of screw-up is just almost unbelievable.

Equifax has known since 2015 that its approach to cybersecurity was lacking, and among other issues, Equifax learned during an internal audit that was conducted that year that the company had left a number of critical and high-risk security flaws unpatched.

The company also learned it lacked the comprehensive IT asset inventory, meaning it would be difficult to address new security issues as they were brought to the company’s attention.

When the Department of Homeland Security informed the public about a major security risk in certain versions of Apache Struts, apparently a very commonly used piece of software, it also told the public that the vulnerability was easy to exploit.

Knowing all of that, Equifax relied on the same flawed policies and procedures which ultimately failed to identify the presence of the vulnerable versions of Apache Struts. Equifax circulated a notice about the vulnerability to an email list that did not include application owners, put the issues on the agenda of two meetings that senior leaders failed to attend regularly, and conducted repeated scans that failed to identify the vulnerability which allowed hackers to access the online dispute portal.

Mr. Begor, if Equifax knew that it lacked a mature inventory of its IT assets, why didn't senior IT and security officials and staff do more to improve the inventory before the 2017 data breach? Specifically, why did Equifax fail to conduct a follow up audit after the 2015 review to determine whether the company had made progress in addressing its patch management issues?

Mr. BEGOR. Ranking Member, I think as you know, I joined in April 2018. In the first few weeks of joining Equifax, I went into great detail to understand the forensics and what caused the breach, what routines and processes were in place at the time. As I stated in my testimony, there were controls in place. They clearly were not strong enough. We have taken great steps since then. We have doubled the size of our security team. I described in my testimony a few minutes ago our increased spending on data and security and our approach to making security central to the DNA of the company.

We also changed the incentives in the company. We are unique in corporate America, I think, that in our annual bonus system, which the top 3,900 out of 11,000 employees participate in, 25 percent of that bonus is tied to cybersecurity. That went into effect in 2018. It has continued in 2019, and it will continue going forward. Ranking Member, that incentive is only punitive, meaning if we do not make progress on our security improvements, if we do not take our security forward, the metric will reduce the individual's bonus, including mine. There is real buy-in to making security a part of our DNA, which we think is quite critical.

I would also say—and I think Mr. Sorenson said the same thing—this will not end, meaning you can never be good enough. The investments and spending will continue, and as I pointed out, we have increased our technology and security spending in 2018, 2019, and 2020 by 50 percent. Security is a top priority at Equifax. It is a top priority of mine, the board, the leadership team, and the whole organization going forward.

Senator CARPER. I spent many years of my life in the Navy—I am a retired Navy captain, a Vietnam veteran—and we have a standard in the Navy and a process in the Navy that says if the captain of the ship is asleep in his or her wardroom in the middle of the night and the ship runs aground, the captain of the ship is held responsible. Has that happened in this case?

Mr. BEGOR. In my view, Senator, it has. I think you know that the prior CEO is no longer with the company. The prior CISO is no longer with the company. The prior CIO is no longer with the company.

If you look at our technology and security organization, we have upgraded really strong talent in approximately two-thirds of both of those organizations. As I talked about, we have added significant resources, approximately 1,000 incremental people since July 2017. We had 10,000 people globally at the beginning of last year. Last year, we added approximately 1,000, and those were all in security and technology. There has been a lot of accountability. Again, I was not there, but there is a new team at Equifax that takes security intensely seriously.

Senator CARPER. Equifax's competitors, which have the same extremely sensitive data on American consumers as Equifax, oper-

ated with a stronger sense of urgency once they learned about the Apache Struts vulnerability. As you assumed the leadership of this organization, you must have wondered, if they are doing this, why didn't we at Equifax? We have asked about what you have done. You explained a bit about what you have done to change the culture of your company around cybersecurity.

If you are advising other companies, whether they happen to be companies that deal in the sort of business that you have, your business model, what advice would you have for those other companies today?

Mr. BEGOR. First, it is a war. I think Mr. Sorenson said the same thing. I think this Subcommittee understands that these criminals that are attacking U.S. companies are increasingly sophisticated. We get attacked multiple times per day, and with the system we have now, I get an alert on my phone from my Chief Information Security Officer and his team when there is an attempted attack on Equifax. Point number one is that this threat is not going away. Point number two is we really applaud the Subcommittee's focus on sharing best practices. As the Senator may know, it is challenging for a company that goes through a data security breach to be open about actually having it. Therefore, I think these forums are critically important.

When I joined Equifax in April, my first call was to my two competitors, and what I told them was that there are no trade secrets around data security. This is a war we face as an industry. It is a war we face for American companies, as you pointed out, for the government, and it is one that is not going to end. We applaud the idea of sharing actively what we are learning from each other. For example, what are the Internet Protocol (IP) addresses that are from known bad actors? If one company knows it, let us make sure the next company knows it and share those so we can really build our defenses up, because the threat is increasingly sophisticated and challenging.

Senator CARPER. I will close this round with this thought. The Constitution of our country was first ratified in Delaware. December 7, 1787, we ratified it before anyone else had. The very beginning of the Constitution started with these words, the Preamble: "We, the people of the United States, in order to form a more perfect union . . ." It does not say to form a perfect union but "a more perfect union." Our goal in this realm has to be perfection, knowing we will never get there, but we need to strive for that.

Thank you.

Senator PORTMAN. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Mr. Chair, and thank you, Ranking Member Carper, both of you, for this investigation but also for your bipartisan leadership of this Subcommittee. Thank you to both of our witnesses for being here today.

Let me start with a couple of questions, Mr. Begor, to you. You said in your testimony you believe that, despite some errors, Equifax took cybersecurity very seriously even before the 2017 breach. I know that the 2017 breach occurred before your time at the helm of the company, but the facts presented in the Sub-

committee's report make clear that the company's pre-breach security practices were really not in keeping with serious cybersecurity practice.

The report shows that Equifax had forgotten to update a security certificate known as an "SSL Certificate" that encrypted data transfers between Equifax's customers and the website.

When Equifax developers attempted to install new certificates, they realized that some of the old ones had expired as much as 8 months earlier. That failure led to the exploitation, as you have acknowledged, of millions of Americans' data by what appears to be Chinese hackers. Equifax should have routinely audited its SSL Certificates to make sure they had not expired, especially since these certificates can only protect user data when they are current.

Let me just ask you a few questions. When Equifax sought to upgrade its SSL Certificates on July 29, 2017, how many expired certificates did your team come across? How many of the certificates had been expired by more than a day?

Mr. BEGOR. Senator, I do not have that information in front of me. If you would like me to, I could ask my Chief Information Security Officer if he could help with that question.

Senator HASSAN. That would be terrific. Thank you.

Mr. BEGOR. OK.

Senator HASSAN. Good morning.

Mr. FARSHCHI. Good morning. Unfortunately, I also was not at Equifax during the time of this incident, and so I do not have that information with me right at this moment. But I am happy to go back to the team to look at—

Senator HASSAN. Does the company have that information?

Mr. FARSHCHI. I believe we do, yes.

Senator HASSAN. Do you know if any of these certificates had been expired for more than 8 months?

Mr. FARSHCHI. Unfortunately, because I was not there, I do not have the specifics regarding the certificates.

Senator HASSAN. I would expect that even though you were not there, that you would know this or have access to it, because it seems to me that is the type of investigation and understanding that you would want to develop moving forward.

Mr. BEGOR. Senator, if I could just add, as you might imagine, we have a much different process today, much more robust, and we know exactly which certificates are expired, which ones are critical. They are risk-rated. We also do automatic scanning as a protocol that would be quite helpful in today's environment. We are continually investing in new technologies to make sure we stay in front of new risks and very rapidly address those.

Senator HASSAN. You are routinely auditing your SSL certificates now?

Mr. BEGOR. Yes.

Senator HASSAN. I am seeing nodding, too.

[Mr. Farshchi nodding.]

OK. You are making sure that they are current and they are not in danger of imminently expiring, correct?

Mr. BEGOR. That is correct.

Senator HASSAN. OK. Would you support a law that would require companies like Equifax that deal with millions of Americans'

personally identifiable information (PII) to adhere to clear cybersecurity standards and practices, such as auditing your security certificates on a continuous basis, standards established by National Institute of Science and Technology (NIST), and enforced through your regulator?

Mr. BEGOR. First, Senator, I agree that Equifax is in a unique position with the data we hold versus most companies. We understand that, and we take it seriously.

With regards to all of the elements you talked about, those are standard protocols for us today and things that we are following as a company, and are the highest standards of data security.

With regards to legislation, we would be happy to work with your office and understand, what is the right legislation to move forward. But we are doing the things you talked about.

Senator HASSAN. I understand you are doing things, but you are doing things after a major breach. What I want to make sure is that Americans whose information is in custody of an entity they may not even know anything about do not have to wait for there to be a breach before companies start doing what they should responsibly do.

We have all discussed that this is an ongoing threat. It has been an ongoing threat for a while now. We need to make sure that there are standards in place just the way we have safety standards in many other industries.

Let me move on just to another aspect of this. It appears from the PSI report that one of Equifax's biggest weaknesses was that the company's policy made individual developers responsible for identifying and patching vulnerabilities in the software they use rather than relying on a full company effort to address any vulnerabilities. As Senator Carper mentioned, unfortunately, when DHS alerted Equifax to an urgent and critical vulnerability in a piece of software called "Apache Struts," the single developer who was using the software was not notified by his superiors about DHS' urgent message about those vulnerabilities. As a result, that developer was unaware of a critical vulnerability that eventually was exploited by hackers.

You mentioned in your testimony that human error was certainly part of the problems that led to the breach, and I think we have all acknowledged that up here, too. However, human error happens at every level of government and every level of the private sector. So it is incumbent upon security professionals and leaders of any security system, government or private sector, to build in extensive redundancies to mitigate against inevitable human errors.

It appears that prior to the breach, Equifax had not built in those redundancies, and as a result, human error became a single point of failure in a critical cyber attack. What redundancies has Equifax built into its system to ensure that inevitable human errors never again lead to this kind of breach?

Mr. BEGOR. Senator, we agree with your summary there that a single point of failure is not ideal which is why we have a number of redundancies. If the Senator is OK, I would ask my Chief Information Security Officer maybe to talk in more detail.

Senator HASSAN. That would be terrific. Yes, thank you.

Mr. FARSHCHI. Yes, one of the key tenets of our program is assurance. We want to make sure we have as many layers of security as absolutely possible because we know that any given control may fail or may be bypassed from a sophisticated attacker.

As it relates to patching, we have updated all of our processes. We have implemented automated tools to be able to help reduce the risk of human error. We have established patch champions, individuals specifically accountable for the implementation of these patches across the entire enterprise. Then we have an automated tracking system to continue to track and manage them.

I would mention one more. On the back end, we continuously scan our environment, so we do not just rely on one system, one process, or one individual. We have a belt-and-suspenders approach across the entire program.

Senator HASSAN. Thank you. That is helpful. I appreciate your indulgence, Mr. Chair.

Mr. Sorenson, I did have a question for Marriott. I will submit it for the record. I want us to be thinking about what kind of standards we should have when companies merge that might help us make sure that we are getting to problems before they occur.

Thank you.

Senator PORTMAN. Thank you, Senator Hassan. We look forward to continuing to work with you on these issues you raised today and others.

I am going to reclaim some of my time now. I will be back with more. To follow up on the points that Senator Hassan made, she talked updating certificates on the website. She talked about building in redundancies. Mr. Begor, you were in your testimony pretty confident that they were doing the right things by saying, "The program also leveraged strong administrative and technical safeguards . . . and was subject to regular, ongoing review through external and internal assessments."

There is a third concern that I have that I think we need to raise this morning and be sure that we are aware of a lack of follow up to an audit that was done. There was a 2015 audit of the security of your system. It found over 8,500 known critical high or medium vulnerabilities on Equifax systems.

Here is an audit that discovers these vulnerabilities. These vulnerabilities had not been patched when the breach occurred, and many of them were over 90 days old. A copy of that audit is there with you on the witness table for you all to look at this morning. I am going to ask that that 2015 audit be made part of the record,¹ without objection.

My question for you is: How does a company that at that time, as you indicated, placed a high priority on cybersecurity allow 8,500 vulnerabilities to exist unpatched on its systems? Of course, my follow-up is: Since you have become CEO and you stepped in and aggressively tried to address these issues, have you addressed these patching vulnerabilities on Equifax's systems? How could that have happened? What has been done?

Mr. BEGOR. Thank you, Senator. As you point out, I was not at Equifax during the breach. I spent quite a bit of time looking at

¹ The information referenced by Senator Portman appears in the Appendix on page 98.

the past. I am a big believer that we want to learn from mistakes and learn from things that were not going as well as they could have been. I will be clear right now that there is no question that what we did in the past, we can do a lot better today and tomorrow, and we already have. We have made significant changes in our security protocols, our infrastructure, and the evolution in the organization. As I mentioned earlier, we brought in really top talent. It starts with people leading these organizations.

I think the Senator may know that the CISO Jamil Farshchi reports directly to me, and also has a line into the board to our Technology Committee, which is a best practice in many companies. We have doubled the size of his team.

With regards to your specific question around audits and patch management, we have also doubled the size of our audit team, and as a new element, we have added IT and cyber experts as a part of our internal audit team. Historically, those were just financial kinds of employees in our audit teams. Now we have experienced technologists and security people in our independent audit teams and are doing some of that work.

With regards to follow up of audits—

Senator PORTMAN. Just hold there for a second. When you look back at the 8,500 vulnerabilities that were reported through that audit, what happened? Why were those vulnerabilities not patched? What was the issue?

Mr. BEGOR. Senator, as you may imagine, a large organization like Equifax has many patches that are underway at all times. They are coming in weekly and daily, and it is part of—

Senator PORTMAN. The race is never won, as was said earlier by Mr. Sorenson.

Mr. BEGOR. Yes, and—

Senator PORTMAN. But the question is: What did you learn from it? In other words, as you look back—I understand that you have beefed up your cybersecurity presence and you have the CISO reporting, and you have put a bonus system in place that incentivizes all your executives to look at it. But what happened? How could those 8,500 vulnerabilities not have been addressed at that time? What did you learn from that?

Mr. BEGOR. I learned Senator, that it is not how you want to operate. We do not operate that way today. There is a real focus on both risk prioritizing and patching so the most critical areas are done first. The next ones happen after that. There is real follow up. There is tracking. I think Mr. Farshchi talked about how we follow up on those. We now have automated systems to track those, but there is a real rigor, as there should be around ensuring that that work is completed and those vulnerabilities are shut down.

Senator PORTMAN. That 2015 audit, if it had been followed up on, would have made a difference, it appears to us, based on our analysis of what happened. Where are you now? Have you done a recent audit? Are you continuing to audit?

Mr. BEGOR. We audit routinely. I do not know—I believe the last audit was done by the internal audit team in the fourth quarter. We also have third parties coming in and doing work around our cybersecurity efforts. We do our own perimeter testing by our own internal team. We also bring in third parties that the internal team

does not know are trying to penetrate the exterior of our system. There are all levels of rigor around getting external inputs like audits around our systems and processes.

Senator PORTMAN. So you have done a follow up audit comparable to that 2015 audit, and you have responded to what has been discovered, because I assume that it also discovered that there were certain vulnerabilities.

Mr. BEGOR. Correct. You want your audit to identify things that will make the system better. That is the way I think about audit teams. I do not know how many audits have been done since the cyber breach in 2017, and I can follow up with your office on the number of audits, but there have been numerous. As you might know, there are also regulatory organizations, the Consumer Financial Protection Bureau (CFPB), the Attorneys General (AG), and others, that are involved in discussions with us around audits, as well as our customers are doing audits.

Senator PORTMAN. Our interest is to figure out, what the heck happened. How could you have an audit that uncovers these vulnerabilities and not act on it? With regard to legislation we are looking at what role should audits play? If you could provide that to the Subcommittee, that would be very helpful, when your last audit was, any results of the audit, how you react to it today, that would be much appreciated. Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you. I want to thank you for bringing this very important, privacy and security. It is issue number one not just for all of us as individuals but for all the companies and businesses that serve us, that we expect to protect us and our communities every single day.

I do have something to talk about, acquisition and data migration. As a former software developer, I have actually done that in my prior life, so I have some comments on that.

But first I want to talk about the global nature, Mr. Sorenson, about Marriott hotels. Of course, you are worldwide. You operate in all 50 U.S. States and in 130 countries and territories. Americans stay at Marriott hotels all over the world, so it is crucial that our data collected is secure. You have noted yourself approximately 23 million passports have possibly been compromised, no matter where the hotel has been physically located.

My question to you is: Last year, Secretary of State Mike Pompeo stated publicly that China was responsible for the cyber attack on your Marriott system and theft of consumer data. Do you believe that to be the case?

Mr. SORENSON. First, good morning, Senator Rosen.

Senator ROSEN. Thank you.

Mr. SORENSON. Nice to be here and to be able to answer your questions. The short answer is we do not know, and I feel quite inadequate about even drawing inferences from the information that we have obtained.

When we first discovered information had been extracted from the system, which was November 19th, it has been all hands on deck basically to make sure that we—

Senator ROSEN. No preliminary data has come out as to where the ISPs may be located or any commonalities in other hacks, other hacking attempts with other companies across the world?

Mr. SORENSON. We have shared everything we have with the FBI, including the addresses used and the malware tools used in the system so that they can do that kind of investigation. We have simply been focused on making sure the door is closed and communicating with our customers.

Senator ROSEN. Do you have policies here in the United States that apply abroad, taking into account, obviously, foreign laws and regulations?

Mr. SORENSON. We do. We have policies certainly about data collection and retention. We also have an obligation to comply with local law. I think one of the things that is unusual about the Marriott cyber attack is this passport information, and the numbers I—

Senator ROSEN. How long do you retain the passport information?

Mr. SORENSON. The passport information that was accessed, again, was in the Starwood reservation system, and it had been there for a number of years.

Senator ROSEN. Do you have a responsibility when you buy a company to do an audit of the company that you are either buying or—I guess it is like buying a home, isn't it? Do you get an inspection? What does the seller disclose? What is the buyer's responsibility? Did you buy it as is so you just took no method of auditing the data coming across?

Mr. SORENSON. The bottom line is we do buy it as is. When you are acquiring a public company and ultimately buy those shares, there is nobody left as a seller anymore. We are Starwood today as well as Marriott. But, of course, we did diligence.

Senator ROSEN. I want to tell you as a former computer programmer, I have worked for companies where I have done this acquisition and data migration, and while the other system is still up, I had a team of people working with me to maintain that system, auditing that system, making sure it had integrity, while we were training and moving that data over.

Where was your responsibility in maintaining and, as you migrated, protecting that data?

Mr. SORENSON. We were very much taking the same approach, so really in three periods we could look at separately. One is the 3½ week due diligence period before we signed documents to acquire Starwood—very abbreviated, public company to public company. That was, "Tell us about your IT system." Our IT team was involved in that and asking questions. But it was quite brief, and we did not learn about any of this.

The second period is between the fall of 2015 and the fall of 2016, between signing and closing the transaction. While we had not closed, our IT team, was deeply engaged in understanding Starwood's system, understanding the data, understanding the vulnerabilities, and being ready essentially for the moment the transaction closed to say, OK, now what are we going to do with this system, both from a cybersecurity perspective, data retention perspective, but also an operating perspective, obviously.

Immediately after closing, it was bringing in not just our internal expertise but external expertise and saying help us identify the risks in this system. Let us make sure we are doing things to address those risks and enhance them. In retrospect, we wish we had done even more. Obviously, something happening.

But even while that system is running independently before the data migration and before it is turned off, we are very much trying to make sure that we are addressing the security flaws that we think are there.

Senator ROSEN. As we think about those 23 million passports and other data that may have been breached worldwide, do you have—I just want to be sure—a consistent policy, of course, taking into consideration certain other governments' laws or regulations, for how you keep the data, how you retain the data, and your responsibility toward the data?

Mr. SORENSON. Let me give you just a couple of data points here, if I could. My number is just a little bit different than the Committee's. About 19 million total passports accessed.

Senator ROSEN. Nineteen or 23, it is an awful lot.

Mr. SORENSON. It is a big number.

Senator ROSEN. It is an awful lot of passports.

Mr. SORENSON. About 5 million of those were unencrypted.

Senator ROSEN. That makes it better?

Mr. SORENSON. No. Those are the ones that obviously would have been—

Senator ROSEN. We know that hackers can beat the encryption, so that is not really a factor here, I do not believe.

Mr. SORENSON. I actually do think part of our strategy going forward is to rely on encryption and tokenization to say whatever data we keep in this space, for example, it should all be encrypted. That by itself is not necessarily a totally adequate defense, but it is one of the tools we should use.

I think one of the other things that is clear, there are dozens of countries around the world that require us to collect passport data. Sometimes they require us to make physical copies of passports for guests in those hotels.

In the Marriott system, legacy, that was done at the hotel level and not centralized in the data platform, if you will.

In the Starwood system, it was done locally and then essentially centralized into the data system.

There are pros and cons of allowing it to be entirely at property level. One of the pros is it is a smaller target, if you will.

Senator ROSEN. That is right.

Mr. SORENSON. One of the cons may be—

Senator ROSEN. It is more diffuse, harder to get centralized.

Mr. SORENSON. That is right.

Senator ROSEN. Much easier to break into and bigger reward.

Mr. SORENSON. One of the cons, on the other hand, is then if each hotel needs the same elaborate system of cyber defenses, can you make sure that you are delivering that? Those are issues we are working through right now.

I think in all likelihood, everything—passports will be encrypted. Second, I think we will look very hard at not centralizing any of

it, but making sure that we have appropriate tools at the proper level to protect against cyber attacks.

Senator ROSEN. Perhaps how long you store customer information, sensitive information like their credit card numbers and those extra security—

Mr. SORENSON. We are looking at that, too, absolutely.

Senator ROSEN. Thank you. I think my time is up.

Senator PORTMAN. Thank you, Senator Rosen. Senator Hawley.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman and Ranking Member, and thank you for having this important hearing. Thank you, witnesses, for being here.

Mr. Begor, let me start with you. You may know that as Attorney General of Missouri, I and 43 other Attorneys General launched a multi-state action after the announcement of the Equifax breach in 2017, and among other things, we sent a letter to Equifax in which we expressed particular concern with Equifax's post-breach activities, including the offering of a fee-based service to guard against data breach at the same time that you were offering a free service. Here is from the letter: "We object to Equifax using its own data breach as an opportunity to sell services to breach victims. Selling a fee-based product that competes with Equifax's own free offer of credit monitoring services to victims of Equifax's own data breach is unfair, particularly if consumers are not sure if their information was compromise."

Can you give us an update on the status of this product? Are you still doing that?

Mr. BEGOR. Senator, thank you for the question. As I mentioned in my testimony this morning, we offered a free product for all Americans, whether they were impacted or not, at the time of the data breach. I do not know the exact timing of when we stopped marketing to consumers, but soon after the data breach—it may have been when we received the letter from you and the other Attorneys General—we stopped marketing to U.S. consumers. We recently started again marketing in October on a very limited basis.

The other thing that we offered in January of—

Senator HAWLEY. But this is a free product, though. You said you were marketing a free product.

Mr. BEGOR. No, Senator. When the breach happened, we offered a free credit monitoring product to any American, and it was opened up to any American whether they were impacted by the data breach or not. That happened in September 2017.

In January 2018, we added another free product for any American that is free for life, that is a Lock & Alert product where, on your mobile device, you can lock your credit file or unlock it. Equifax is the only credit bureau offering that.

Last, you talked about marketing to consumers. We stopped marketing in the—I do not know the exact date; I can come back to your office—but in the fourth quarter of 2017 to U.S. consumers.

Senator HAWLEY. What about the fee-based product, however, that you were offering after the announcement of the breach?

Mr. BEGOR. That is what I was referring to, Senator. We stopped that in the fourth quarter of—

Senator HAWLEY. You stopped marketing it——

Mr. BEGOR. That is correct.

Senator HAWLEY [continuing]. In the fourth quarter. OK.

We raised a number of other concerns, the Attorneys General, in that same letter and in that same multi-state action, including the terms of service that required customers to waive their rights, charges customers pay for a security freeze with other credit monitoring companies, and overly long wait times for the Equifax customer support call center. Can you give us an update on how you have addressed these concerns?

Mr. BEGOR. Yes, Senator. On the freezing your credit file, I referred to what Equifax proactively did in January 2018 offering a free lock product to any American, and that is still offered today. You can get that today. I have it on my phone. It allows you to lock or unlock your credit file at no charge and it's free for life.

As the Senator also knows, last September the Senate passed S. 2155 that offers consumers free freezes for life. That was passed, and that is in place, and we have implemented that along with the other two national credit bureaus.

With regards to our customer service center, there were clearly some challenges there as I look back on what happened in the fourth quarter. Staffing up for something like the breach response is challenging. In my testimony this morning, I talked about the incremental \$50 million of investment we are making now in our customer service capabilities to enhance our abilities to manage our day-to-day interactions with consumers as well as investing to make it easier for consumers to interact with us when they have a question, outside of a data breach but just in their normal day-to-day activities with the credit bureau, whether it is around a dispute or a question on their file.

Senator HAWLEY. Thank you.

Mr. Sorenson, in the testimony you have provided, the written testimony you have provided to this Committee, you noted—and I am going to make sure I get this right. You noted that you have not received any substantiated claims of loss from fraud attributable to the incident, and that none of the security firms that you have engaged to monitor the Dark Web have found evidence that information contained in the affected tables has been or is being offered for sale, and that you have not been notified by any banks or credit card networks that Starwood had been identified as a common point of purchase in any fraudulent transactions.

Do you take this to be a thorough accounting of which sources might know about your customers' data used by third parties? Is it sufficient for you just to wait for them to report to you?

Mr. SORENSON. I think the answer certainly to the first question is no. It is hard to feel like anything is thorough in this space. You pick up signals from a number of different places. We use a number of different tools, for example, to try and go after the same thing.

We take some comfort in this, but it is only some comfort. I think we are grateful for the partnerships we have with the financial institutions so we can have a little bit of that dialogue about what they might be seeing. But, one of the reasons we put the WebWatcher out and made it available to our customers is that it

is another tool to look regularly at the so-called Dark Web to see whether a particular customer's information is showing up on that Dark Web.

Senator HAWLEY. If I could just press a little deeper here, in your written testimony does this reflect an ad hoc list of sources that could report this information about personal information of users? Or does this reflect some sort of cybersecurity methodology that you have in place in order to protect your consumers' data?

Mr. SORENSON. No, I do not think this is really in the first instance about protecting consumers' data. I think it is about assessing what we can assess about the cyber breach that occurred. If you will, the attack happened—successful, I suppose, if you take it from the attackers' perspective. Information was obtained. We have been wrestling with the consequences of that. One of the tools that we are using is to try and figure out, OK, what can we tell about where that data has ended up.

The tools that we use to protect the data in the first place I think are different and in many respects I would say much more fundamentally important, because we want to avoid that data from getting out in the first instance at all.

Senator HAWLEY. You do have some cybersecurity methodology that you have now put in place to systematically protect your consumers' data? That is what you are telling me?

Mr. SORENSON. A whole range of tools.

Senator HAWLEY. My final question here, Mr. Chairman. Are you complying with General Data Protection Regulation (GDPR), Mr. Sorenson? I understand that GDPR in Europe requires reporting within 72 hours if at least one Marriott customer resides in the European Union (EU). Is that your understanding as well?

Mr. SORENSON. Yes, and we believe we are.

Senator HAWLEY. Thank you, Mr. Chairman.

Senator PORTMAN. Thank you, Senator Hawley.

Senator Harris.

OPENING STATEMENT OF SENATOR HARRIS

Senator HARRIS. Thank you. Thank you, Mr. Chairman, for bringing this subject up. As California's AG, I supported expanding California's laws as it relates to the requirement of the report of data breaches and have met with many folks over the years who have suffered greatly because of the breach of their personal information and data. The risks are obviously many.

Mr. Begor, Equifax is facing lawsuits from consumers whose information was affected by the breach. In response, your lawyers have argued that even though their information was stolen, consumers cannot prove that they were harmed. It was recently reported that none of the data stolen from Equifax in 2017 has been used in identity theft or other fraudulent activity and that the stolen data has not been offered for sale on the Dark Web.

Do those assertions remain true?

Mr. BEGOR. They do, Senator Harris. To date, we use a variety of outside experts as well as our own, like Marriott, to try to understand where the data went and what it was used for. Our analysis is that there has been no evidence that the data has been sold and

no evidence of increased identity theft as a result of Equifax data that was stolen in 2017.

Senator HARRIS. A former senior intelligence official recently told CNBC that the hack was more likely the work of a foreign intelligence agency than a garden variety criminal, which would explain why the stolen information has not been used for garden variety crimes. If a foreign power, especially a hostile foreign power, is using the data it stole from Equifax to target U.S. officials or American operatives, does it remain your position that there has been no injury or harm caused by this breach?

Mr. BEGOR. Senator, we do not know who took the data, and we still do not, and we are working closely with the FBI. Days after identifying the cyber breach in 2017, we started collaboratively working with the FBI and other authorities. We have the same goal. We have been completely transparent about who took the data, and we just do not know who it is at this stage. We continue to work with those authorities.

Senator HARRIS. It would be important for us to know that you appreciate the fact that if the data were breached for the purposes of gaining information about U.S. officials or American operatives, there would most certainly be harm and damage and injury that would result from that. Do you appreciate that concern?

Mr. BEGOR. Of course, Senator. In my testimony this morning, I started out by expressing regret for what happened. I talked about what we are doing for consumers, which was our initial focus and continues to be our focus around supporting consumers, the free credit monitoring that we offer, the other free products that we have rolled out subsequent to the data breach around supporting consumers.

Senator HARRIS. Do you understand that there have been targeted violations of privacy as it relates to employees of the U.S. government and that there is a concern among the intelligence community (IC) and all of us that there is a focused concern and actually a triangulation around officials, American officials, and, in particular, those who may be involved in our military or in intelligence work, and the attempt being to get their personal information for the purposes of attempt to compromise those individuals? Are you aware of that concern?

Mr. BEGOR. I have read and I have listened to the experts who we work with about the threat on American companies and on American consumers as well as government employees.

Senator HARRIS. Will you commit to this Committee that you will have that as a priority among your priorities in understanding and thinking about the potential harm that has resulted from these breaches?

Mr. BEGOR. Senator, I testified this morning that security is a top priority at Equifax today. We have doubled our security team.

Senator HARRIS. Is that yes?

Mr. BEGOR. The answer is everything we are doing is around yes.

Senator HARRIS. OK. Great.

Mr. Sorenson, as Senator Rosen referenced, in November 2018 hackers exposed the personal information of up to 383 million Marriott customers, including millions of passport numbers. Shortly after, cybersecurity firms and recently our government was hired

to assess the damage attributed to the hack and attributed it to Chinese intelligence. In addition to passport numbers, could hackers have accessed guests' itineraries and the names of their traveling companions?

Mr. SORENSON. Yes—well, traveling companions I am not certain about, but reservation data was obtained, I think most recently as far as we can tell in 2016, so that would have been my upcoming reservation or perhaps a past reservation that I had had at one of the Starwood hotels. We do not think, based on what we have been able to tell so far, that any reservation data post-2016 was obtained by the cyber attacker. In the 2018 instance, which was the first one after we acquired Starwood, we do not think individual reservation data was there.

This is not 100 percent provable, but we believe that that means there is no longer any upcoming reservation data which was obtained, because if 2016, 2 years—we tend not to take reservations more than a year out. Probably nothing that is still, if you will, a future reservation.

Senator HARRIS. As it relates to the names of traveling companions, it is the custom of Marriott hotels to collect the information of whoever is occupying the room, whoever has the credit card plus whatever guests they may have. Isn't that correct?

Mr. SORENSON. This is the Starwood reservation database, and certainly in many instances, a hotel would note somebody else who might be sharing a room, but not necessarily in every instance. If the person who made the reservation is showing up and checking in and getting the key, the front desk may or may not take the time to make the effort to figure out whether a spouse or a child or somebody else was traveling with them. But certainly it would have happened in some circumstances.

Senator HARRIS. For those folks whose names may have been exposed but they are not actually the individual who was contracted with the hotel to pay for the room, have those people been notified of this breach?

Mr. SORENSON. We tried very hard to notify everybody that we could. The first tool we used, of course, was a broad press release with broad public dissemination, and then carrying on the banner, if you will, the top line of the Marriott.com, Starwood.com apps, all the rest of it.

In addition, we sent out in excess of 50 million emails to folks that we had email addresses on to also make sure that we were notifying them in that way.

Is it possible that somebody has slipped through the cracks? Of course. I think the more likely that they were repeat customers of ours, the more likely they are travelers, the more likely that they would have been either notified by us directly or seen the news.

Senator HARRIS. Mr. Chairman, just one last question and it is a brief question.

Is it correct that Marriott is the top hospitality provider for the American Government and the United States military?

Mr. SORENSON. I do not know that we have the data which would tell us that. We are the largest hotel company by rooms—

Senator HARRIS. Can you follow up with the Committee and see if you may have the answer to that question?

Mr. SORENSON. I will ask and see whether we can find out, yes.
 Senator HARRIS. Thank you.
 Senator PORTMAN. Thank you, Senator Harris. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Thank you, Mr. Chairman. Thank you to our witnesses today.

Mr. Begor, if a consumer is delinquent on a payment but later makes the necessary payment to bring the account current, it is my understanding that that delinquency stays on the credit report for 7 years. Is that correct?

Mr. BEGOR. Yes, it is, Senator.

Senator PETERS. If a consumer misses a single credit card payment and then you will continue to follow them for basically 7 years, and then they are going to have an opportunity to in that 7 years basically demonstrate that they are a good credit risk, a good credit score, and as a result of that then get additional credit as a result of that after that 7-year period. Is that correct? If there is not any other activity?

Mr. BEGOR. There is not, Senator. But as you may know, in the credit scoring models that we and other credit bureaus use, using your example if there was one delinquent payment, as that ages out, it becomes less predictive—has less impact on an individual's credit score and ability to obtain credit.

Senator PETERS. But, still, it is the expectation it takes 7 years—you want to watch it for 7 years, basically, just to see how it acts. Obviously, there is a slope there. I bring that up because I think that most people—certainly everybody that I talked to believes that Equifax was beyond being just delinquent on one payment when it came to the securing of this critical data and this cybersecurity hack, and that the information that has now been put out or has been taken will likely be there forever. The fact that you have not seen some of these activities in the short run may make sense because if you are a bad actor, you may wait a while before you actually use this data for nefarious purposes.

I just find it kind of interesting in that delinquent payments for a consumer you follow for 7 years although you have offered the credit freeze for a lifetime, when it comes to credit monitoring it is only 2 years. Credit monitoring is certainly much more preferable to consumer convenience than it is to freeze and to unfreeze, to go back and forth. I know you want to build consumer trust, but if you are telling your consumers, we will watch you for 7 years because you have missed one payment, but we had this massive breach, and we gave all your personal information, somebody got all your personal information to millions of people and it is going to be out there for the rest of your life, but we will help you for 2 years.

It seems to me that it would make sense that at a minimum you would offer credit monitoring for the 7 years just as you monitor your customers for 7 years.

My question to you, Mr. Begor: Would you support mandating free credit reporting for 7 years for all consumers whose personally identifying information (PII) was the subject of a breach of a credit reporting agency?

Mr. BEGOR. Senator, we think it is situational on what the consumer should be offered. We offered 12 months starting in the fourth quarter of 2017. We voluntarily extended it for another 12 months late last year. We will continue to look at that as we go forward. Again, it is my view that legislation is not required, that we are doing the right thing for consumers.

I would just remind the Senator that while the credit monitoring is a valuable product, what the Senate passed last September in S. 2155 offering a free freeze for consumers is the most important way to protect your data. Then Equifax has a supplemental lock product that is available on your phone or mobile device that is free for life to do the same thing with some more functionality. If you are at a car dealership and getting an auto loan, you can unlock your credit file. Then when you finish getting that financial transaction, you can lock it again. No one can see that data once it is either frozen by S. 2155 or locked by our free-for-life product.

Senator PETERS. But you still see the value of monitoring because you are offering it to your customers for up to 2 years, that that is a better product for folks than just the freeze and unfreeze, which is more cumbersome. I think you mentioned that at the beginning.

My question is what—you said you will re-evaluate this on a situational basis. What is that situational basis? What is the criteria you will be using as to whether or not to extend this beyond the 2 years?

Mr. BEGOR. Senator, it really depends on how we can see the data have been used and what they are being used for. These are some of the criteria we take into account. I would make the point that while credit monitoring is quite valuable, we believe that it is critically important to give consumers control about who has access to their data.

Senator PETERS. I would like to in the remaining time touch briefly on another important subject, and that is the collecting of data on minors. How many minors had their personally identifiable information compromised in the 2017 breach?

Mr. BEGOR. Senator, I do not have that information in front of me. I would be happy to get back to your office with that.

Senator PETERS. Is it greater than zero?

Mr. BEGOR. I do not know the answer to that, Senator.

Senator PETERS. You will provide that to me?

Mr. BEGOR. Yes.

Senator PETERS. That would be great.

Do you have any policies regarding the collection of information on minors?

Mr. BEGOR. The policy is that we do not. As you may know, S. 2155 allows a parent to put a freeze on their children's credit file, if, in fact, they have one. We are diligent about managing minors' freezes because it is an area of focus by impostors or fraudulent individuals who want to create a credit file for identity theft purposes not only on minors but other Americans.

Senator PETERS. Is there any instance where a young child would need a non-frozen account?

Mr. BEGOR. Not to my knowledge, Senator.

Senator PETERS. But a parent has to opt out even though there is no reason to have a non-frozen account. But the parent has to be active in doing that. OK.

Last year I worked to pass legislation that protects children from synthetic identification (ID) fraud. It is a form of identity theft that I know you know very well where stolen security numbers of children are paired with fake names and birth dates to apply for loans, credit cards, and other accounts. Could any minors' information that was exposed in the 2017 breach be used as part of identity theft or a synthetic ID fraud operation?

Mr. BEGOR. Senator, I will have to get back to you on what minors' data were included, in the theft that took place in 2017.

Senator PETERS. Great. Well, I appreciate working with you on that.

Thank you.

Senator PORTMAN. We will have a short second round. Senator Carper, do you have any additional questions?

Senator CARPER. Both Equifax and Marriott publicly announced their data breaches within weeks of learning of them, and while this is better than some companies have done in recent years, as you know, it is a lot longer than, for example, Target waited when it suffered a breach in 2013. In fact, Target learned about a cyber attack, you may recall, affecting its customers in the middle of holiday season—I was one of them that year—and informed the Department of Justice (DOJ) and the public literally within days, and this allowed Target customers to take precautions against fraud and identity theft and to monitor their bank and credit card statements.

Mr. Begor, the hackers who attacked Equifax were in the company network for 78 days before Equifax discovered their presence. I think that is correct. By the time Equifax informed the public, consumers' information had been in the hands of hackers for close to 4 months.

Given the damage that can be done with the type of information Equifax collects, why do you suppose the folks who were in positions of responsibility prior to your arrival, why wait 6 weeks to step forward? Why not follow the Target example so that people could take swift action to protect themselves as soon as possible? If I had been you coming into a new situation as the new CEO, I would have said to the people who were there before me, "What were you thinking? How could you have allowed this to happen?" Did you ever have those kinds of conversations?

Mr. BEGOR. Senator, I had a lot of conversations when I joined last April, as you might imagine, and I hope you get a sense for the pace of change, the breadth of change, the priority around security. There is a whole new team here. We have added extensive resources, and we are very serious about security.

With regards to the time frame with the data breach, my strategy—and I believe it was the team strategy at the time—was to be accurate and quick in completing the work. As the Senator probably knows, it is a very complex process once you find out that you have a data breach to really determine which elements of your database were affected. We brought in the very best forensic experts within days of the data breach—I think it was a day or two—

contacted the FBI and got them involved in it. From my look back at what the team did, they moved as quickly as they could to ensure that we were going to be complete and accurate.

From my perspective, making an announcement that there was a data breach but not knowing which Americans were impacted, and is it 50 million, 2 million, 150 million, it took time to do the forensics to figure it out. My approach is to be accurate and complete with a real focus around the consumer first. We want to make sure that for those consumers who are impacted, we can identify who they are and then communicate with them quickly.

Senator CARPER. Mr. Sorenson, really the same question. I would like to hear from you about the factors that went into Marriott's decision on the timing of its public notice.

Mr. SORENSON. An alert on September 7, 2018, was triggered. That alert went to a third party who was operating the reservation system for us with, in effect a copy to the IT group at Marriott. We heard from that third-party operator the next day, on September 8th, that that alert had been received and immediately started to mobilize resources to contain and to ascertain why that alert went off.

It was not until November 19, 2018, that we learned that data about our customers had been exfiltrated from our system. We announced publicly 11 days later on November 30th.

We, of course, had lawyers and security experts and all sorts of other folks who were engaged in the conversation about timing, how quickly could we go. We also wanted to make sure that we had set up call centers and websites so that the moment we released this information publicly, the customers had a place to go and find out more and sign up for the WebWatcher services and do the other things that were necessary.

That 11-day time, of course, met the legal requirements, but it also was practically about as fast as we could move it and be able to communicate something which was concrete and useful to customers and then be able to deliver something of what we anticipated they would need and want.

Senator CARPER. Thank you. Let me just ask both of you do you have any sense of how many State data breach notification laws your companies are subject to? Would it be fair to say there may be even 50 such State laws that you are subject to at this time?

Mr. BEGOR. If it is OK, Senator, I will go first. You are correct and it is quite a challenge in—

Senator CARPER. I was going to ask, what kind of challenge does that present if it is true?

Mr. BEGOR. I do not know if the exact number is 50, but they are all different, and it creates challenges in a situation like Equifax, as perhaps Marriott's too, in complying with the requirements. There are different notification documents that are required. There are different ways you may communicate with a consumer. There are different ways you are allowed to communicate with the consumer. We have been longstanding supporters of Federal legislation that would unify the requirements and ensure there is a consistent time element. Once you figure out which consumers are impacted and what States they are in, then there are require-

ments in how you must communicate with them. We are very supportive of a Federal legislation to unify the standards.

Senator CARPER. Thank you.

Same question, Mr. Sorenson. What kind of challenge do you have with respect to who to notify, when to notify, what to disclose about a data breach with the different States?

Mr. SORENSON. It was not among the biggest challenges we faced, I would put it that way, although if memory serves, we found someplace between 20 and 30 States had specific notification requirements with a deadline. Now, we, of course, met those deadlines and then ultimately communicated to all 50 States.

Outside the United States, there were probably, I do not know, 20 or 30 countries that had various kinds of notification deadlines. Obviously, there is nothing that the Federal Government can do with that.

Sadly, I suppose, in some respects, this ground is too well trod, and so there are folks that can help us figure out where those requirements are and how to meet them.

It would be simpler, of course, to have one sort of U.S. standard, but, that is something that we would be happy to work with your office on and give whatever input we could from the experience we have had.

Senator CARPER. Mr. Chairman, I am sitting here thinking, believe it or not, of something Richard Nixon of all people once said. Richard Nixon once said, "The only people who do not make mistakes are people who do not do anything." We all make mistakes. I have said to my sons now, 29 and 30 years old, I have said to them many times, "Nothing wrong with making a mistake. The key is just we do not want to continue making the same mistake."

In this case, mistakes not only harmed your companies, but as we have talked about, they harm 150 million really innocent people across this country.

The question is: What do we do about it? You have talked to us today about a number of things that each of you have done. I am pleased to hear the statements of apology, of contrition, acknowledging the harm and the damage that has been done. God knows I wish, as I am sure 148 million people wish, that the kind of thinking and actions that you have displayed in the last year or so that you have been in your position, Mr. Begor, that that kind of thinking had existed in the previous Administration, if you will.

You talked about what I think is really important. Leadership is most important in grading the success of any organization I have ever been a part of, business, government, or military—always the key. If the leader does not say cybersecurity is important, if the board does not say cybersecurity is important, nobody else down the line is going to make it important in the end.

It appears to us that you have done that, both of you, and have made it very clear right from the top that this is important. You have aligned incentives, financial incentives, for the folks who are helping run your company so that their incentives are all lined up with that in mind. It sounds like you have done a lot with respect to hiring the kind of workforce that you need to enable the desires and the wishes of the directives from on top to make sure that they are carried.

One of the things that I think a lot about, Mr. Chairman, is the workforce—I know you do, too. We have focused in Delaware for a number of years now—at the University of Delaware, Delaware State University, Wilmington University, and Delaware Technical Community College—on trying to make sure that we are turning out a better workforce to help take on all these jobs that are available out here to be done.

With regard to the Federal Government and what our responsibilities are, I was privileged to chair this Committee, the Homeland Security and Governmental Affairs Committee, for a while and led it with a fellow named Tom Coburn from Oklahoma, and we focused this Committee—as Senator Portman knows, he was part of this—on what we needed to do within the Federal Government and what we needed to do as legislators. Frankly, in those years, those couple of years, we did a lot, and we have continued to do a number of things. I really think, Mr. Chairman, that this is a ripe time for us as a Committee. We have new talent on either end here, Democrat and Republican, bright people with real-world experience that can bring a lot to this. I think it is really an ideal time for us to do our job of oversight. We have done all this legislating, and it is being implemented. Let us find out to what effect, to what good. That is a big part of our job.

The last thing I will say is I would ask to enter for the record some newspaper articles¹ I read on the train coming down this morning from the last several weeks about the dramatic increases in attacks from China and from Iran. I remember when President Barack Obama met with President Xi in Washington State. You may remember this. It was 2015. I think it was September 2015. Jeh Johnson, who was the Secretary of Homeland Security, gave me his eyewitness account, and in that meeting, President Obama apparently said to President Xi, “We know you are attacking us, and we know that you are coming after our trade secrets. We know you are coming after our business secrets, our military secrets, and we want you to stop.”

President Xi apparently said, “No, we do not do that. That is not the policy of our country, and that is not what we are about.”

President Obama basically said, “This is who is doing it, this is where they are located, and we want you to stop.”

President Xi said, “No, we are not really doing that.” I am told that President Obama said, “Look, if you do not stop, you will wish you had,” essentially in so many words.

As you may recall, there was a dramatic drop in attacks by China.

About 2 months before that, the Congress, the United States, and the President had essentially signed off on a five-nation deal with Iran that called for gradually lifting sanctions. At the time Iranian elements were unrelentingly attacking, especially our financial services companies. I was a strong supporter of lifting sanctions in return for the Iranians stopping their development of nuclear weapons and opening up to incredible, very intrusive inspections, and they are still ongoing. You know what happened? Lit-

¹The newspaper articles referenced by Senator Carper appears in the Appendix on page 108.

erally within a month, the frequency of Iranian attacks greatly dropped, almost like China a couple of months later.

There is another element here, Mr. Chairman, that we do not think much about, and there is so much that they can do, so much that other companies can do and need to do. There is work for us to do in terms of creating the workforce and making sure they are available. There is stuff that we can do in our oversight role. But there is also a role here for the Administration in reaching out to other countries and getting them to work with us instead of being out there undermining what we are trying to do.

There is plenty of work to do, a multilayered approach, and we appreciate your being here today and helping to put a spotlight on this, letting us know what you have done to clean up the messes that you inherited, especially at Equifax. It has given us an opportunity to think ourselves how we can better do our own jobs. Thank you. Because everything we do, everything I do, I know we can do better, and that certainly includes this.

Thank you.

Senator PORTMAN. I cannot believe government can do anything better than it is doing. Well, thank you.

To the witnesses, I have two follow up questions here that we want to get into the record, but let me reiterate what I said earlier, which is we appreciate your being here. We are trying to learn. The lessons that you have learned within your companies are really important for what we are trying to do legislatively, understanding what happened, what could be done differently.

This was frightening, scary, for hundreds of millions of families whose personal and financial data was compromised through the two companies you now lead. I appreciate the fact that you acknowledge that and understand that this is about hackers, it is about technology, but it is ultimately about people. The frustration that many Americans have right now that nothing is sacred or safe and it is good to know, as Mr. Sorenson has said and Mr. Begor has said, that some of this data apparently has not been used yet by criminals in ways that one might have thought it could have been. That does not mean it did not happen or is not happening right now.

Also, as was raised earlier, some of this information may be being used by foreign actors in ways that are counter to our national interests by targeting individuals. It is really important that we get to the bottom of what happened, what is being done, and what can be done in the future legislatively.

Let me go back, if I could, to the cybersecurity protocols, Mr. Begor, that we talked about earlier. In your testimony you seem to have leaned a little bit heavily, I thought, on the fact that the program at the time, I said, "leveraged strong administrative and technical safeguards . . . and was subject to regular, ongoing review through external and internal assessments." We talked about the audit that was not respected despite some really troubling data it uncovered.

The other part that I think we need to talk about this morning—and I was waiting to hear what my colleagues were going to address, and they addressed a lot of this, but that is the IT inventory. The investigation, as you know, found that Equifax at the time

failed to follow this basic practice of maintaining an IT inventory of applications and assets on its systems. Without having this list, Equifax was not able to find the application that was vulnerable and exploited by the hackers. That is the one that has been talked about previously called “Apache Struts.” You did not even have it on your inventory, and so you could not find it. I guess I have a few questions.

One, since the breach, has Equifax generated a comprehensive list of applications on its systems?

Mr. BEGOR. We have, Chairman, and in great detail, and I think my colleague Mr. Farshchi talked about some of the other automated systems that we put in place to track all of our systems and make sure we understand not only the systems and all the assets that we have, but also when there is a patch that needs to be completed, those are all automated, and we are watching them. Then there are multilayers of defense. It is more than just one layer. I think the Chairman knows that all the elements have to be done well and done with the latest technology, which is what we are continuing to put in place.

Senator PORTMAN. The National Institute of Science and Technology, has now issued a recommendation that there be an IT inventory in every company that could be affected by these breaches. Let me ask you this: If Equifax had kept an up-to-date IT inventory, would that have been helpful to have identified the vulnerability?

Mr. BEGOR. In my analysis of what happened in 2017, there was an inventory. It was not as complete as it should be. The protocols and the procedures and the resources we now have in place are at the highest standards. Like most companies, we follow the NIST protocols, and as I mentioned earlier this morning, Chairman, we have third parties actually auditing us against those NIST standards as a part of how we are managing our security program going forward.

Senator PORTMAN. We have a difference of opinion on that. Our investigation identified that there was not a complete inventory. Mr. Farshchi, maybe you can respond to this, but was there an inventory or not? Did that affect the ability to find the vulnerability?

Mr. FARSHCHI. Certainly. Inventory is an important control across any organization to defend against the threats. I was not here at the time, but looking back, we did have an inventory. It just was not a complete inventory. Since that time, what we have done is we have built in those controls, as Mr. Begor was saying, and so we do have a complete inventory of our assets. And note that—

Senator PORTMAN. It sounds like, if I am right, that you did not have a complete inventory and Apache Struts was not something that was able to be identified. Is that accurate?

Mr. FARSHCHI. What I would say is this: The inventory for Apache Struts is typically not in the inventory that you highlight in the report, and it is a technical nuance. But the specifics of that particular vulnerability typically are not included in the asset inventory. Because it is a source code vulnerability, it is typically in a code repository instead.

Senator PORTMAN. We have a little difference of opinion on this one, so we follow up with you. Again, it is about the future going forward. Are you telling me that something of the nature of Apache Struts would not be in your current inventory and, therefore, you would not be able to find that vulnerability today?

Mr. FARSHCHI. No; it absolutely is in our inventory.

Senator PORTMAN. It should be in the inventory?

Mr. FARSHCHI. It is just it is a different type of inventory, Senator.

Senator PORTMAN. OK. Well, if they had had in the inventory that they were reviewing, clearly it would have made a difference. Do you agree with that statement?

Mr. FARSHCHI. Made a difference with respect to what, Senator?

Senator PORTMAN. The ability to find the vulnerability.

Mr. FARSHCHI. It would have helped.

Senator PORTMAN. Thank you. OK. Mr. Sorenson, thank you for being here, too. I want to follow up on one of the points that we found in our investigation. It is true the big breach happened at Starwood in 2014. Then you acquired Starwood in 2016. Is that correct? Then in 2018, you were able to identify that something had happened. You said the alert was issued in 2018.

However, we have not mentioned today there was a 2015 breach at Starwood that was acknowledged, and so when you bought Starwood, you knew about—I assume you knew about that breach. Is that correct?

Mr. SORENSON. Yes, we did.

Senator PORTMAN. That breach was a credit card breach. Numbers were taken at points of sale at 54 different properties, and January 22, 2016, to be exact—the president of Starwood sent a public letter out saying that the guest reservation database was not impacted by that breach. I have a copy of that letter there at the witness table for you. I would like to enter that 2016 letter into the record,¹ without objection.

Of course, in reality, the reservation system had been breached considerably in 2014. The letter said do not worry, reservation system has not been breached.

My question to you is just a simple one: When you did your due diligence, which you talked about having done, did you look at that letter, and did you examine this issue? Could you have determined, therefore, earlier what happened?

Mr. SORENSON. It is a very fair question. The short answer is we knew about the point of sale breach that Starwood has suffered. We worked with the Starwood team and we worked independently to try and make sure we understood the scope of that breach.

As far as we know today, it was totally unrelated to the reservation system breach that we have been talking about announced in November—different tools, a different system. In a sense, the point of sale is obviously distributed at the properties and the restaurants and at the front desk. The reservation system, by comparison, which was the larger breach we disclosed in November, is a centralized system. Again, the team has said they do not relate to each other, although certainly from a colloquial perspective, it

¹ The letter referenced by Senator Portman appears in the Appendix on page 106.

feels similar, it feels like a warning. It feels like somehow it is relating to Starwood's customers, which it is.

We did try and understand that point of sale thing, and we were satisfied that Starwood had taken the steps necessary in order to deal with that breach. Separately, we did some things on the reservation platform side, but it was in retrospect clearly not enough.

Senator PORTMAN. Well, lessons learned, and we appreciate the testimony you have already given us, and we appreciate the opportunity to stay in touch with you and your experts to help to be sure that we are putting together the kind of legislation that can help avoid these problems in the future.

You made a statement earlier. This is a race that has no finish line. I think that is accurate. I think it is also accurate that this is a marathon that has to be run at a sprinter's pace because there will be continual innovative hacking. I noticed this morning, to Senator Carper's point, that while the President was in Hanoi in negotiations with Chairman Kim, there was an increase apparently—this is a report, take it as such—in North Korean hacking, commercial hacking of U.S. targets. It is something that we are going to have to continually assess, and government is not often good at that. We put a law in place, as Senator Carper said. We do not do the proper oversight and follow up, and we sometimes get behind the curve. We want your ongoing cooperation with this panel to be able to put together what makes sense and then to update it as necessary, because you are going to both be in your companies engaged in this for a long time into the future.

Thank you again for being here.

Senator CARPER. Mr Chairman, just a unanimous consent (UC) request, if I could, to enter for the record articles from February 16th, New York Times,¹ "Chinese and Iranian hackers renew their attacks on U.S. companies"; and the Wall Street Journal is I think as recently as yesterday, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years." I would ask they be considered and included in the record.

Thank you.

Senator PORTMAN. Thank you all for your testimony.

Senator CARPER. Thanks to all of you.

Senator PORTMAN. OK. We will now call our second panel of witnesses for the hearing. Please come forward and take a seat.

This is the expert panel that is going to give us information about how to solve so many of the problems we just talked about. We welcome you. We are going to start by introducing the panel.

Alicia Cackley is here with us. She is Director of Financial Markets and Community Investment at the Government Accountability Office (GAO). We appreciate GAO's work on this issue and on this report.

Second, we have Andrew Smith with us, who is Director of the Bureau of Consumer Protection at the Federal Trade Commission (FTC).

¹The New York Times articles referenced by Senator Carper appears in the Appendix on page 108.

Third, we have John Gilligan with us. Mr. Gilligan is the president and chief executive officer at the Center for Internet Security (CIS).

Again, it is the custom of the Subcommittee to swear in all witnesses, so at this time, I would ask you to stand up again and raise your right hand. Do you swear the testimony you will give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. SMITH. I do.

Ms. CACKLEY. I do.

Mr. GILLIGAN. I do.

Senator PORTMAN. Please be seated. Let the record reflect that all the witnesses answered in the affirmative.

Your written testimony will all be made part of the record, so if you could keep your oral presentation to 5 minutes, that would be great. Mr. Smith, I think we told you you would go first, so we are going to call on you first.

**TESTIMONY OF ANDREW SMITH,¹ DIRECTOR, BUREAU OF
CONSUMER PROTECTION, U.S. FEDERAL TRADE COMMISSION**

Mr. SMITH. Thank you. Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, I am Andrew Smith, the Director of the Bureau of Consumer Protection at the Federal Trade Commission. I appreciate the opportunity to present the Commission's views on how Congress can help the FTC further its efforts to prevent data breaches in the private sector.

My written statement represents the views of the Commission, but this opening statement represents my views alone and not necessarily the views of the Commission or of any individual Commissioner.

Let me begin by summarizing the FTC's current efforts to protect consumers by promoting data security and preventing data breaches.

Our work has three primary areas of focus. The first is enforcement. For nearly two decades, the FTC has been the Nation's leading data security enforcement agency. We are charged with enforcing data security requirements contained in specific laws such as the Children's Online Privacy Protection Act (COPPA), Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA). But we also enforce Section 5 of the FTC Act, which prohibits unfair or deceptive practices, including unfair and deceptive practices with respect to data security.

In this law enforcement role, the Commission has settled or litigated more than 60 actions against businesses that allegedly failed to take reasonable precautions to protect their customers' personal information. For example, we have brought cases against manufacturers of consumer products like smartphones, computers, routers, and connected toys. We have also brought cases against companies like data brokers that collect consumers' sensitive personal information.

Our second area of focus is policymaking. The FTC has conducted workshops, issued reports, and made rules to promote data

¹ The prepared statement of Mr. Smith appears in the Appendix on page 69.

security. For example, just this week we announced a Notice of Proposed Rulemaking (NPR) to update our Safeguards Rule under the Gramm-Leach-Bliley Act. The Safeguards Rule was originally issued in 2002 and requires financial institutions within the FTC's jurisdiction to implement reasonable process-based safeguards to protect personal information in their control. The proposed revisions to the Safeguards Rule are based on our nearly 20 years of enforcement experience. These revisions are intended to retain the process-based approach of the original rule while providing financial institutions with more certainty with respect to the FTC's data security expectations.

Our third area of focus is business education. The Commission has issued numerous guidance materials for business, including a guide called "Start with Security" in 2015, a series of columns in 2017 called "Stick with Security," and last year, a comprehensive small business cyber education campaign, which includes written guidance, how-to videos, and training materials for businesses. These materials distill the lessons learned from our enforcement actions in a succinct and accessible manner. We have vigorously used our existing authority to protect consumers, but this authority is limited in some important respects, and the Commission has called on Congress to enact comprehensive data security legislation that includes rulemaking, civil penalty authority, and enhanced jurisdiction for the FTC.

First, the legislation should give the FTC the authority to issue data security rules under the Administrative Procedures Act (APA) so that we can keep up with business and technological changes. Where we currently have rulemaking authority, we have used it, as demonstrated by this week's proposed revisions to the Safeguards Rule, which I just described.

Second, legislation should allow the FTC to obtain civil penalties for data security violations. Currently, we have authority to seek civil penalties for data security violations under the Children's Online Privacy Protection Act and the Fair Credit Reporting Act. We also can get civil penalties for violations of an existing administrative order. But as a general matter, we cannot obtain civil penalties in de novo cases. To help ensure effective deterrence, we urge Congress to enact legislation to allow the FTC to seek civil penalties for data security violations in appropriate circumstances.

Finally, the legislation should extend the FTC's jurisdiction over data security to nonprofits and common carriers. Entities in these sectors often collect sensitive consumer information and significant breaches have been reported, particularly in the educational and nonprofit hospital sector.

Thank you for the opportunity to appear before you, and I look forward to answering your questions.

Senator PORTMAN. Thank you, Mr. Smith. Ms. Cackley.

TESTIMONY OF ALICIA PUENTE CACKLEY,¹ DIRECTOR, FINANCIAL MARKETS AND COMMUNITY INVESTMENT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. CACKLEY. Thank you, Chairman Portman, Ranking Member Carper. My name is Alicia Puente Cackley, and I am a Director in the Financial Markets and Community Investment Team at the Government Accountability Office. I am pleased to be here today to testify about Internet privacy and data security issues.

My statement will discuss the Federal Trade Commission's role and authorities for overseeing Internet privacy and stakeholders' views on potential actions to enhance that Federal oversight. My testimony is primarily based on our January 2019 report on Internet privacy as well as prior GAO reports on various privacy issues.

As you are aware, the United States does not have a comprehensive Internet privacy law governing the collection, use and sale, or other disclosure of personal information. In prior work, we have found that gaps exist in the Federal privacy framework, which does not fully address changes in technology in the marketplace. At the Federal level, FTC currently has the lead in overseeing Internet privacy using its statutory authority under Section 5 of the FTC Act to protect consumers from unfair and deceptive practices.

However, to date, FTC has not issued regulations for Internet privacy other than those protecting financial privacy and the Internet privacy of children, which were required by law.

For FTC Act violations, FTC may promulgate regulations, but is required to use procedures that differ from traditional notice and comment processes and that FTC staff said add time and complexity.

Stakeholders GAO interviewed had varied views on FTC's oversight of Internet privacy. Most industry stakeholders said they favored FTC's current approach: direct enforcement of its unfair and deceptive practices statutory authority, which they said allows for flexibility. Other stakeholders, including consumer advocates and most former FTC and the Federal Communications Commission (FCC) Commissioners GAO interviewed, favored having FTC issue and enforce regulations.

Stakeholders identified three main areas in which Internet privacy oversight could be enhanced.

First, through statute. Some stakeholders told GAO that an overarching Internet privacy statute could enhance consumer protection by clearly articulating to consumers, industry, and agencies what behaviors are prohibited.

Second, through rulemaking. Some stakeholders said that regulations can provide clarity, fairness, and flexibility.

Third, through civil penalty authority. Some stakeholders said FTC's Internet privacy enforcement could be more effective with authority to levy civil penalties for first-time violations.

Recent data breaches at Federal agencies, retailers, hospitals, insurance companies, consumer reporting agencies, and other large organizations highlight the importance of ensuring the security and privacy of personally identifiable information collected and maintained by those entities. Such breaches have resulted in the poten-

¹ The prepared statement of Ms. Cackley appears in the Appendix on page 79.

tial compromise of millions of Americans' personally identifiable information which could lead to identity theft and other serious consequences.

These recent developments regarding Internet privacy and data security suggest that this is an appropriate time for Congress to consider comprehensive Internet privacy legislation. Although FTC has been addressing Internet privacy through its unfair and deceptive practices authority and FTC and other agencies have been addressing this issue using statutes that target specific industries or consumer segments, the lack of a comprehensive Federal privacy statute with specific standards leaves consumers' privacy at risk.

In our January 2019 report, we recommended that Congress consider developing comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving Internet environment. Issues that should be considered include: which agency should oversee Internet privacy; what authorities agencies should have for that oversight, including notice and comment rulemaking authority and first-time violation civil penalty authority; and how to balance consumers' need for Internet privacy with industry's ability to provide services and innovate.

Mr. Chairman and Ranking Member, this concludes my prepared statement. I am pleased to respond to any questions you may have.

Senator PORTMAN. Thank you for your testimony and your help on this issue. Mr. Gilligan.

**TESTIMONY OF JOHN GILLIGAN,¹ CHIEF EXECUTIVE OFFICER,
CENTER FOR INTERNET SECURITY**

Mr. GILLIGAN. Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, my name is John Gilligan. I serve as the Chief Executive Officer of the Center for Internet Security, a nonprofit cybersecurity organization. In my oral statement this morning, I would like to share my perspectives on the logical question that may be asked after this morning's testimony, which is: What can be done to prevent major cybersecurity breaches?

I asked myself a similar question in the early 2000s as the Chief Information Officer of the United States Air Force (USAF) after the National Security Agency's (NSA) annual penetration analysis found our cybersecurity posture to be woefully inadequate, despite the Air Force spending literally over \$1 billion a year on cybersecurity. I went to NSA and asked them: Where should I start?

After consulting their offensive and defensive experts, NSA came back with a prioritized list of the system weaknesses that were most commonly exploited by attackers. By a large margin, the most common weakness exploited was misconfigured software, that is, software that did not have appropriate security settings enabled or software that was not properly patched. As a result of their guidance, I launched an initiative in the Air Force to ensure security-enabled configurations with up-to-date patches for all of our operating systems.

¹ The prepared statement of Mr. Gilligan appears in the Appendix on page 90.

Based on the positive experience with the Air Force in identifying most frequent cyber attack patterns and the associated mitigating security controls, the NSA effort was subsequently adopted by the private sector in 2009 and became known as the “SANS Top 20.” In 2015, the effort was transitioned to my current organization, the Center for Internet Security, and what became named the “Critical Security Controls,” or just the “CIS Controls.”

The Critical Security Controls represent a set of internationally recognized prioritized actions that form the foundations for basic cyber hygiene or effective cyber defense. The controls are regularly updated by a global network of cyber experts. The Critical Security Controls have been assessed as preventing up to 90 percent of pervasive and dangerous cyber attacks. The controls act as a clear, actionable, and free blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order.

CIS has analyzed major data breaches over the past 2 years and have found in each one the root cause of the breach related to the failure to properly implement one or more of the Critical Security Controls. The Equifax breach is no exception. We found that 5 of the 20 Critical Security Controls were not properly implemented by Equifax.

Many organizations are seeing the value of the Critical Security Controls. California, Ohio the Republic of Paraguay, the European Technical Standards Organization—have adopted the controls as a standard for cybersecurity. The Aerospace Industries Association and the Atlantic Council have also endorsed the Critical Security Controls.

As Congress considers ways to improve cybersecurity in the United States, I offer the following recommendation. I start with the recognition that the NIST Cybersecurity Framework is an excellent top-level guidance document that points to other more detailed documents and best practices for implementation guidance, including the Critical Security Controls. While a logical construct, this approach has some unintended consequences. In particular, government and private sector organizations who wish to implement the NIST Cybersecurity Framework must then select for implementation from among the very comprehensive lists of standards, guidelines, and best practices that are referenced in the Framework.

This same problem is magnified for organizations that are required to comply with multiple high-level frameworks that are similar to the NIST Cybersecurity Framework. For example, financial organizations are required to certify against the Payment Card Industry (PCI), security framework. Organizations with international presence are often required to follow the International Standards Organization (ISO), cybersecurity frameworks and so on.

While the individual policies and regulations are well intended, they are contributing to much confusion and inefficiency in achieving the common goal of effective cyber defense.

Recognizing that our multiple cybersecurity frameworks and duplicative policies have contributed to great confusion, I would recommend that NIST be chartered to develop a single cybersecurity implementation guideline that can be used to satisfy the require-

ments of the NIST Cybersecurity Framework, PCI, ISO, Institute of Electrical and Electronics Engineers (IEEE), and similar general security frameworks. This implementation guideline should provide clear guidance on what constitutes basic cyber hygiene and specify a prioritization for implementation of appropriate controls. I note that the United Kingdom and Australia have done exactly this with the Australian Signals Directorate's "Essential Eight" and the United Kingdom National Cyber Security Center's "Cyber Essentials." I offer the Center for Internet Security's Critical Security Controls as a point of departure or a model for such an effort.

This concludes my remarks. I look forward to your questions.

Senator PORTMAN. Thank you, Mr. Gilligan. Thanks to all three of the witnesses. As we heard this morning, these data breaches have become a fact of doing business, haven't they? It is a matter of constantly keeping up. It never ends.

The best estimate we have, the most recent data we have comes from the first half of 2018, and that is there were 291 data records compromised every second. I do not think that has slowed down. It has probably increased. It is an ever present danger to consumers, to businesses, to our government, and to our national security.

Mr. Smith, I found your testimony interesting. As has been alluded to today, 50 States have different stands on this. Most States have passed their own breach notification laws. In fact, I think every State has some sort of breach notification law, don't they, Mr. Gilligan?

Mr. GILLIGAN. I believe that is the case.

Senator PORTMAN. Yes. That is good but they vary significantly from State to State. Let me ask you this, Mr. Smith: What benefit would there be from having a single standard at the Federal level for breach notification legislation given, again, this climate we have of increased technological interconnectedness and the number of breaches we are seeing?

Mr. SMITH. Right. It seems like there would be some benefit to uniformity. I should, though, say that our current Commission, as you know, is composed of five Commissioners. All of them are new within the last year or so, and they have not had an opportunity to testify on whether or not they would support a uniform data breach notification standard. Past Commissions have supported such a uniform notification standard.

Senator PORTMAN. But in your personal capacity this afternoon, what is your opinion?

Mr. SMITH. I was interested, actually, by what Mr. Sorenson said when he said, yes, it was a challenge, but it was not necessarily their primary challenge. I worked at the FTC in the early 2000s, and at that time California had passed its first-in-the-Nation data breach notification standard. We dealt with it under the ChoicePoint breach, which was a huge breach at the time. We started looking at whether we should have a uniform standard, and, in fact, the Commission, I believe, testified in favor of it at that time. Bills were introduced in 2006 to say we need a national standard, every State is going to enact their own standard. Well, every State has, and the sky has not fallen.

I feel as though companies have probably figured out how to comply. I do have to say that I think there is always a benefit to uniformity in terms of ease of compliance. But from what I can tell in the market, companies seem to be able to comply with this multiplicity of standards.

Senator PORTMAN. Ease of compliance is one issue, and I do think that is something we will hear about from the private sector that they would prefer to know what the standards are and not to perhaps even inadvertently not follow a standard that is different State to State. But beyond that, it is about protection. It about the consumer.

Mr. SMITH. Right.

Senator PORTMAN. It is about the government's security and so on. Do you think there is some benefit to that, in other words, having a high standard that we can, therefore, ensure we have better security?

Mr. SMITH. One of the critical aspects of any kind of a breach notification standard is the trigger for notification. I think that in the earlier panel it was mentioned that there is a 72-hour notice requirement in GDPR. From the perspective of someone who focuses on consumer protection, I want to get notices to consumers that are useful, that give actionable—

Senator PORTMAN. Accurate.

Mr. SMITH. Accurate, give them actionable information. I think the worst thing—and we have seen it in some of these breaches—is piecemeal notification. One notice goes out, “Oh, we thought that was breached, and you should do this in response.” Then another notice goes out, “Oh, we have discovered this other asset was breached.”

Senator PORTMAN. This adds to the frustration that people already feel.

Mr. SMITH. It adds to the frustration. You need to give a company time to investigate. They have to investigate quickly. Give them time to investigate, figure out who was affected, and what information was compromised and what consumers can do to protect themselves as well as develop the systems to respond—the 800 lines, the credit monitoring, things like that. So, 30 days, 45 days, something like that. The FTC has a rule that applies to breaches of certain health care information where the standard is as quickly as possible, but in no event longer than 60 days. I do not know if that is the right cut or not, but you need to give people a little bit of time to conduct a thorough investigation.

Senator PORTMAN. I do not disagree with that, but I think 60 days is excessive given—

Mr. SMITH. Could well be.

Senator PORTMAN [continuing]. The fast-moving nature of this and the potential for people's information to be compromised.

On the Administrative Procedures Act, I noted you talked about that in your oral remarks. I think the Administrative Procedures Act rulemaking probably does give us more flexibility. In other words, as I said earlier to the previous panel, we want to be able to respond quickly to a changing threat because it is going to be evolving. However, there is concern that unless it was specifically

related to rulemaking authority for cybersecurity legislation, it could get out of hand.

Can you speak to that for a moment? One, do you think rules under the APA are necessary, and do you think that will add to flexibility? Second, how do you narrow it to being sure that it is responsive to the congressional actions we might take on this one issue?

Mr. SMITH. Right. The Commission has testified in favor of APA rulemaking for data security only. I think what folks imagine would be a bill like several that we have seen introduced, where Congress says, Companies, you shall assess risk and develop a plan to keep data safe and maybe provide some other boundaries for what the program ought to look like, and, FTC, you shall have rulemaking authority under the Administrative Procedures Act, to execute only that law, right? Not APA rulemaking authority for everything in the world.

What we have right now—and it was referred to by Ms. Cackley—is rulemaking authority under the Magnuson-Moss Warranty Act, which requires us not only to do Notices of Proposed Rulemaking and taking of comments; we have to do Advanced Notices of Proposed Rulemaking. We have to have hearings. We have to issue interim reports. We have to allow for interim appeals.

What that means—it is not impossible to do, but what it means is that, from soup to nuts, a “Mag-Moss” rule takes us 10 years.

Senator PORTMAN. Yes, it slows down the process considerably.

One final point, and then I will go to Senator Carper. On the nonprofits you mentioned, you said that private carriers and nonprofits should be under the FTC rubric for this purpose. Can you give us a couple of examples of that? I am thinking about hospitals where there had been some breaches as an example where sensitive medical information could be released inadvertently sometimes, sometimes through hackers.

Mr. SMITH. Right. Hospitals are the issue. If it is medical information, health care information, and it is a hospital, then that will be covered by Health Insurance Portability and Accountability Act of 1996 (HIPAA), and we work closely with the Department of Health and Human Services (HHS) and the Office of Civil Rights (OCR) to enforce and administer HIPAA standards.

What we have seen with nonprofit hospitals are breaches of employee data, not covered by HIPAA, and that is a real challenge. We have also seen breaches at educational institutions. We have seen breaches at common carriers, and there is, I think, a bit of an open question about the Federal Communications Commission’s authority to address those.

Senator PORTMAN. Jurisdiction over that, yes.

Mr. SMITH. Jurisdiction to address those breaches.

Senator PORTMAN. Thank you. All things to look at. Senator Carper.

Senator CARPER. Thank you for your really illuminating testimony this morning. You were sitting out in the audience, and I do not know what you were thinking about, but you came to the table prepared, and it is very much appreciated.

One of the things that is always helpful to me when we have a panel of well-informed, thoughtful witnesses is to see where do you

think you agree, and the question would be: Where do you think you agree as a panel with respect to what Congress should do next? Would you just start us off, Ms. Cackley?

Ms. CACKLEY. Senator, I think where certainly my testimony and Mr. Smith's testimony were in agreement was around the need for legislation and what some of the elements of that legislation could include, which is to say notice and comment rulemaking authority, civil penalty authorities. Those were the things that would best help the FTC or whichever agency Congress chooses to invest with this issue, oversight over this issue, the necessary tools to be able to get the job done.

Senator CARPER. All right. Thank you.

Mr. Smith, where do you think the three of you agree on what we should be doing next, our to-do list, if you will?

Mr. SMITH. Particularly with respect to the statutory authority for the Federal Trade Commission to make rules in the area of data security and enforce using civil penalties and also the expanded jurisdiction, we certainly agree on that. I agree with Mr. Gilligan from CIS about the importance of these useful rubrics like the CIS Critical Security Controls to educate businesses and to focus their attention on things that really matter. For a lot of businesses, I think that data security is sort of an insurmountable obstacle. It is beyond anyone's comprehension. These types of rubrics I think help businesses to focus their attention in the right place.

We have done the same thing this week with our GLBA Safeguards Rule. The rule began in 2002 and at the time was quite influential, but it is very basic. It requires companies to have good data security, conduct data assessments, and appoint people to be responsible. In our new rule, which is somewhat longer, we offer more specifics about encryption and penetration testing and some of the other best practices, which provides businesses with an auditable standard, provides them with clear information about our expectations, and also, candidly, provides us with more ability to enforce.

Senator CARPER. Mr. Gilligan, same question. Where do you agree?

Mr. GILLIGAN. I think there is fundamental agreement that this is a complex issue. There are a number of regulatory bodies—Federal Trade Commission being one—who have jurisdictions over parts of our economy. One of the functions that the Center for Internet Security provides is what we call the “Multi-State Information Sharing and Analysis Center,” where, under funding from Congress and under DHS sponsorship, we provide security support for State, local, tribal, and territorial governments.

Included in State, local, tribal, and territorial is almost every different domain that you might imagine, and they are all struggling dealing with cybersecurity. While I am personally not an expert in data breach reporting, I can say that the States and local governments are struggling trying to deal with all of the well-intended regulations that I mentioned in my testimony. I think some consolidation of that and simplification and, as I suggested, perhaps using something like the Critical Security Controls as the technical implementation foundation. That is where most organizations need relief—and that needs to be continuously updated. That is what

most organizations need help to focus on the problem, and as I said, the breaches that have been discovered invariably are the result of failure to implement very simple controls in a comprehensive way.

Senator CARPER. I asked my staff to gather a handful of tips for consumers, for regular folks, to follow if they become a data breach victim, and the short list—it is not a comprehensive list, but one of those is change your password. Another would be to contact your bank or your credit card company. A third would be to contact a credit reporting bureau. A fourth would be to sign up for credit monitoring. That is for folks who had become a breach victim.

Mr. Gilligan, what would you suggest that consumers can do to protect themselves prospectively, not after they become a victim but prospectively? Any tips?

Mr. GILLIGAN. I think it would be largely parallel to the list you just mentioned. One of the things that I would recommend is that all consumers freeze their credit reporting, which is often a vehicle through which their particular personal information is compromised.

I think having good hygiene with regard to passwords, with regard to software updates and use of security software are also things that all consumers should do on a regular basis in order to protect themselves.

Senator CARPER. Mr. Smith, Ms. Cackley, anything you want to add to that list?

Mr. SMITH. I would direct consumers to our website, FTC.gov, where we have a tremendous amount of information about how to protect yourself in the event of a data breach, both general information as well as specific information. For example, we have pages that are dedicated to tax identity theft. We have a page dealing with connected toys. Just a couple of months ago, in December 2018, there was a phishing scam where consumers received what appeared to be authentic emails from Netflix saying, “You need to provide us with your payment information again.” We developed a specific page or consumer education to deal with that because it was an important threat to consumers.

We also built pages for the Marriott breach and the Equifax breach that gave specific information for consumers who had received those notices about what they could do to protect themselves, including some of the measures that your staff mentioned.

Finally, when consumers believe that they may be a victim of identity theft, they need to go to Identitytheft.gov, which is operated by the FTC, and there we have tools such as the identity theft affidavit that you can use with the credit bureaus to have fraudulent information removed from your credit report, as well as receive other rights under the Fair Credit Reporting Act.

Senator CARPER. All right. Thank you.

Ms. Cackley, one last word?

Ms. CACKLEY. I would say just that consumers need to educate themselves, thinking prospectively. They need to understand what data is potentially available to other people, what companies are collecting their data, and how they can set privacy controls potentially or do whatever else they can to keep themselves safe.

Senator CARPER. Terrific. Thank you. You had to wait here for a while in order to share your thoughts with us, but for us it was well worth the wait and we thank you very much.

Senator PORTMAN. I cannot tell you how much we appreciate your testimony and also the ongoing work with us on this because we have some real expertise here.

By the way, with regard to the FTC—I think I speak for Senator Carper on this, too—we really want you to feel responsible. In other words, one of the concerns that I have had is there is so much of this going on, breaches, some of which relate to private companies, some, as you mentioned earlier, nonprofits. Many people are concerned about where their information is going, even if it is not a business per se that you would normally think of as we saw in the earlier panel, but even any of these websites where, you are giving information and that information is then being given out to other people. Folks want to know about it. I hope—and maybe Ms. Puente Cackley can do some work on this going forward—that you all feel empowered to be that one stop for a consumer. If they have a concern, they can go to your website and figure out both what is going on with the specific issue, as we talked about earlier, if there has been a breach at a big company and, they can find out what the information is about how they can protect themselves, but also just general information.

I assume you feel you have that responsibility already, but we want to be sure that whatever legislation we do squarely puts that responsibility, frankly, and accountability on the FTC. Any thoughts on that?

Mr. SMITH. We are the country's only general jurisdiction consumer protection agency. Of course, we have a lot of consumer protection agencies—the Food and Drug Administration (FDA) or the Securities and Exchange Commission or the banking agencies. We are the only ones who take a general view to the whole marketplace, and we believe that should Congress pass legislation with respect to data security or privacy, we are the agency that is best equipped to enforce and administer that statute, not only because of our more than 20 years' experience with privacy and data security—in fact, if you look at the Fair Credit Reporting Act, which has been around since 1970, and we have been in charge of enforcing and administering it—but also just our general know-how with respect to how to protect consumers and our focus on consumer harm, whether it is deceptive practices or unfair practices. We have the goods to show for it, right? We have brought 60 cases plus in the data security area and the same in the privacy area.

Finally, I would say that I think that, unlike an agency that has specific jurisdiction, I think we are less susceptible to capture. If you look at the more than 100-year history of the FTC, we have proven remarkably immune to that, and I would worry about a special agency dealing with privacy in terms of the potential for regulatory capture.

Senator PORTMAN. I think that is consistent with where we would like to go with legislation just to affirm that and to make sure there is a clear line of responsibility.

My final question is about Ohio, of course, and it is to Mr. Gilligan, because he mentioned Ohio in his list of States and coun-

tries that have put in place some kind of an Internet security control system. We have recently in Ohio established our Center for Internet Security Controls as a standard for cyber defense after passing the Ohio Data Protection Act. Could you discuss briefly the role of the CIS controls within the Ohio Data Protection Act and how legislation of this kind can incentivize companies to implement some of these baseline cyber controls we have talked about today?

Mr. GILLIGAN. Thank you, Senator. The Ohio legislation is ground-breaking legislation in that for the first time it provides specific guidance with regard to expectations for cybersecurity. As you mentioned, it does reference a couple of the Federal guidelines, specifically it references several NIST documents. But the Critical Security Controls is only one of the references that really provides specific implementation guidance, and so we believe that that is the type of guidance that is required.

As you know, the Ohio legislation is voluntary, and the intent of it is really to provide positive incentives to those doing business within Ohio to improve their status of cybersecurity, and we think that is sort of the right way to go, to provide a clear definition of what are the expectations, encourage through positive rewards organizations to comply with those best practices, and to serve as an example for industry as well.

Senator PORTMAN. Thank you, Mr. Gilligan. Senator Carper.

Senator CARPER. Mr. Chairman, before we close, I just want to thank a couple members of our staff from the majority side and the minority side by name and insert for the record the names of some other folks who have worked on this. We have been at this for a while. There are some people who have come and gone, and I want to just have those names entered for the record: on the majority staff, Andy Dockham, and Patrick Warren, especially for their hard work, and there are others, I know, as well.

On the minority staff, I want to thank Roberto Berrios, Brandon Reavis, Meeran Ahn, and John Kilvington; our law clerks, Conor Daly, Justin Azar, and Taylor Burnett, who helped prepare for this hearing. We have a number of folks, former staff, former law clerks, who have gone on to other pursuits, but we are grateful to them. We will enter those names for the record. We are only as good as the people we have behind us, and we are blessed by the folks that sit behind us and help us.

Senator PORTMAN. Thank you, Senator Carper. I thank the witnesses for their testimony this morning. Both panels I thought were very informative. I also want to thank your staff, Senator Carper, and you for leading on this important issue of protecting consumer information. That is how we work here. It is a non-partisan approach, and my staff also deserves recognition for doing a great job in working with our witnesses and others to make sure this was a thorough investigation.

As with our other investigations, we are going to be looking at legislation, so we want your continued help on that. I look forward to working with Senator Carper on that.

The hearing record will remain open for 15 days for any additional comments or questions by any of the Subcommittee Members, and with that, this hearing is adjourned.

[Whereupon, at 12:32 p.m., the Subcommittee was adjourned.]

APPENDIX

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.

**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.

Written Testimony of Mark Begor
Chief Executive Officer of Equifax Inc.
U.S. Senate Committee on Homeland Security & Government Affairs
Permanent Subcommittee on Investigations
March 7, 2019

Chairman Portman, Ranking Member Carper and distinguished members of the Subcommittee, thank you for the opportunity to be here today. I am Mark Begor, Chief Executive Officer of Equifax, a role that I accepted in April 2018 after 37 years in senior leadership roles at General Electric and Warburg Pincus. With me today is Jamil Farshchi, who joined Equifax in February 2018 as our Chief Information Security Officer (CISO), reporting directly to me. Mr. Farshchi is a seasoned security expert and brings significant and relevant information security experience to Equifax, having previously served in senior information security roles at The Home Depot, Time Warner Inc., Visa, Los Alamos National Laboratory and NASA.

While I was not a part of the Equifax team when the cybersecurity incident occurred in 2017, I certainly recognize the disruption and impact that the cyberattack caused for U.S. consumers and our customers — and I deeply regret what happened. I also understand that our regulators and lawmakers undoubtedly felt, and continue to feel, a strong duty to ensure that the financial ecosystem is functioning in a way that benefits consumers and safeguards their personal data.

Cybercrime—targeting individuals, our nation’s businesses and our government—is one of the greatest threats facing our country today. U.S. corporations are continually attempting to combat criminals that operate outside the rule of law and attempt to extract data for their own gain. In 2018 alone, it is reported that over 1,200 data breaches occurred at U.S. companies. These attacks are no longer just a hacker in the basement attempting to penetrate a company’s security perimeter but instead are carried out by increasingly sophisticated criminal rings or, even more challenging, well-funded nation-state actors or military arms of nation-states. These attacks on U.S. businesses are attacks on U.S. consumers and attacks on America. Fighting these attackers will require partnership and cooperation among government, law enforcement and private business. Since discovering the breach in 2017, we have been committed to transparency and open best-practice sharing with our competitors, with our customers, with the U.S. government and across U.S. industry. This war is getting more challenging and more sophisticated and will not end.

We have cooperated with the Subcommittee and appreciate the significant time and resources it has spent in conducting its investigation. At your request, Equifax has undertaken an extensive production of documents, responded to dozens of interrogatories, and produced and coordinated both internal and external experts to brief your staff. It has been our intent to be transparent with you and with the public about the circumstances surrounding our breach.

As we have previously shared with the Subcommittee, the cybersecurity incident announced on September 7, 2017 occurred because criminals exploited a vulnerability on Equifax’s online

consumer dispute portal to steal information. Our forensic review estimated that the criminals stole certain personally identifiable information of approximately 148 million consumers. Although the data stolen was sensitive, including names, social security numbers and dates of birth, there is no evidence that the perpetrators accessed the financial credit report information of any consumer. Of note, to date, we have not identified any evidence indicating that the information stolen from Equifax in 2017 has been sold or any evidence of increased identity theft. We continue to monitor the dark web and other sources for evidence of the stolen data being used in a criminal fashion.

While I was not with Equifax when the cyberattack occurred or when it was announced, I understand that both technology failures and human errors contributed to the breach. However, the fact that Equifax did not have an impenetrable information security program and suffered a breach does not mean that the Company failed to take cybersecurity seriously. Before the cyberattack, I understand that the Company's security program was well-funded and staffed, based on a robust set of policies, standards, and procedures, and supported by general and specialized training. The program also leveraged strong administrative and technical safeguards overseen by a CSO and was subject to regular, ongoing review through external and internal assessments.

In April 2018 when I joined Equifax, I made a personal commitment internally and externally to build a culture within Equifax where security is a part of our DNA and committed that Equifax would be an industry leader in data security. I am proud of the leadership, cultural enhancements and investments that Equifax has made over the past 18 months and our progress toward being an industry leader in data security.

In those 18 months, we've had a meaningful refreshment of our Board of Directors, with four new directors (including me) joining the Board. The Board is regularly updated by our CISO about cybersecurity matters and our security transformation progress. Equifax has a mindset that everyone at the Company must have an understanding of and appreciation for the role they play in keeping our environment secure — and the Board is no exception. In fact, our CISO has developed a Board Cyber Audit Framework that consists of a set of programmatic and operational metrics so that directors can better understand where the company stands with respect to cybersecurity and so that any issues that arise are treated with the proper urgency. Equifax intends eventually to share this framework with other companies as a tool to leverage with their own boards to increase awareness about important cyber topics that boards and management teams regularly face.

Last year, we made senior-level appointments on my leadership team to help round out our strong security, data governance, IT and risk management teams. As already noted, I joined Equifax in April of last year. I have a deep understanding of the financial system and the importance of credit reporting agencies to that system, having served as CEO of GE's retail credit card business as well as a Director of FICO. In addition to hiring Mr. Farshchi as CISO, we also appointed Bryson Koehler, the former Chief Technology Officer at IBM Watson and Cloud Platform, as our new Chief Technology Officer. We have made other significant additions to

our team, including Nick Oldham as Chief Privacy and Data Governance Officer and Kent Lindner to lead our Enterprise Risk and Compliance functions.

These leadership changes are helping drive accountability from the top down as we work to strengthen our holistic culture of security. But to truly transform into an industry leader, we must embed security into everything we do — from product development, to our merger and acquisition strategies, to our incentive compensation plans. To that end, in 2018, we implemented a company-wide security goal in our annual bonus for the 3,900 bonus eligible employees across the company. This sort of ‘shared-fate’ mindset reinforces accountability and properly incentivizes our workforce — regardless of role or department — so that security is viewed as a responsibility not only of the security team, but also of the entire company.

Another component of our culture change includes a concerted effort to attract and cultivate the best and brightest cybersecurity talent because, ultimately, our success or failure hinges on our people. In 2018, we added nearly 1,000 full-time IT and security professionals to our workforce. We sought highly-specialized, technical talent that will help Equifax develop a world-class security organization.

We recognize that part of being an industry leader in data security is being transparent about our learnings over the past 18 months and actively sharing the best practices that we are collecting as we implement change. Nearly every day we read about new data breaches in the media, impacting a wide-range of industries and companies. All security practitioners stand to benefit from information sharing and open dialogue. Therefore, in 2018 we established a number of meaningful cyber forums and partnerships that ultimately will raise the bar for the entire security community. We founded ATLAS, a public-private sector initiative aimed at sharing threat intelligence and thought leadership, and we were invited to join the World Economic Forum’s Centre for Cybersecurity. We also joined the Better Identity Coalition and are taking a leadership role in policy discussions to reduce reliance on the Social Security number and to support a secure digital identity. We plan to continue this level of investment and initiative in 2019 and beyond.

The last part of our plan to implement meaningful change in our organization includes the technical improvements we are making to strengthen the maturity of Equifax’s security program. We are dramatically increasing our security and technology spending by an incremental \$1.25 billion between 2018 -2020 and will spend approximately \$1 billion per year during this timeframe to transform our technology and security into industry-leading capabilities.

In 2018, we enhanced our core information security competencies, matured the program to address current and future environmental changes, and began to regain consumer and customer trust. Among our most important achievements were the following:

- Implemented a 24 x 7 x 365 follow-the-sun Security Operations Center, enabling Equifax to better respond to cyber incidents in real time and in many cases with local resources.

- Established a data discovery program and deleted unnecessary data and records, reducing the footprint of high-risk systems.
- Reinstated the majority of compliance certifications that were suspended as a result of the cybersecurity incident.
- Deployed updated identity and access management controls with enhanced security being applied to thousands of privileged, administrative and service accounts and restricted administrative privileges on hundreds of endpoints.
- Completed penetration testing of hundreds of externally-facing applications – those with the highest propensity for being attacked.
- Increased code security scanning, with each code scan representing an opportunity for developers to identify and remediate security flaws prior to moving their code into production.
- Created technical assurance measures to validate control effectiveness.

We will continue our record levels of investment in our security and technology in 2019 and 2020. Heading into 2019, our technical project portfolio looks to further increase maturity by executing against key security considerations such as controls assurance, acquisition integration and cloud services. We will continue to be transparent about our lessons learned.

In addition to setting a goal of being an industry leader in data security, Equifax has been working diligently to support U.S. consumers. When Equifax announced the cyberattack, Equifax's response was guided by a desire to do everything it could—going well beyond the requirements of data breach notification laws and doing more than other companies facing major breaches had done—to help consumers. While the rollout of these services was not flawless, Equifax worked diligently and invested substantial resources to mitigate any impact on consumers. Since the 2017 incident, Equifax has spent more than \$90 million on supporting consumers.

At the time the incident was announced, Equifax rolled out a suite of services to assist consumers, including a call center staffed 18 hours a day, seven days a week and a dedicated, consumer-facing website. We offered all American consumers—regardless of whether they were affected by the incident—the opportunity to enroll for one year, for free, in our TrustedID Premier service, an identity theft protection and credit file monitoring service. TrustedID Premier included three bureau credit file monitoring, identity theft insurance, internet scanning for Social Security numbers, the ability to lock and unlock Equifax credit reports and copies of Equifax credit reports. In November 2018 when that service was nearing its conclusion, Equifax voluntarily decided to extend the protection for another year.

Equifax also has taken an industry-leading role to give consumers more control over personal credit data. In January 2018, Equifax launched the Lock & Alert™ service to allow consumers to quickly lock and unlock their Equifax credit reports for free, for life, using a simple mobile application that we developed. Additionally, following the 2017 incident, Equifax provided U.S. consumers the ability to freeze and unfreeze their Equifax credit files for free, and, in

September 2018, we successfully implemented the national security freeze requirements included in S.2155, the “Economic Growth, Regulatory Relief, and Consumer Protection Act.”

At the same time, Equifax took an extra step and unveiled a new online consumer enrollment center called myEquifax™ to make it easier and more convenient for consumers to manage their credit information online. To date, more than 600,000 consumers have taken advantage of myEquifax to more easily manage their security freezes or fraud alerts. Our roadmap for myEquifax includes significant additional investments to help consumers process and manage disputes on their credit reports, including sending proactive alerts to consumers on the progress of their disputes. This new service will help give consumers transparency and peace of mind that their disputes are being handled promptly and with urgency. We are investing an additional \$50 million in 2019 and 2020 to enhance our consumer facing capabilities and will continue our focus on ensuring that we are consumer friendly at every touchpoint.

To close, I would like to assure the Subcommittee that Equifax is committed to working collaboratively with Congress as we continue to find ways to combat cyber crime. I have been clear since I joined Equifax last April that we are committed to becoming an industry leader in security and to becoming more consumer-friendly. We are investing unprecedented amounts in technology and security, as well as enhancing our processes to make it easier for consumers to manage their credit reports. And, as you have heard, we are bringing the best resources and people to Equifax. Every U.S. company, consumer and government agency is facing a relentless attack by cyber criminals. This is a war that will not end. Continued investment in industry-leading data protection technologies and open collaboration to share best practices are our only defenses.

While we still have more work to do, please know that we remain open to sharing best practices with our peers and partners and to making sure that the millions of consumers who need credit to power their financial dreams are treated fairly and with respect and that they have a consistently positive experience with Equifax.

Thank you again for the opportunity to provide this testimony, for your dedication to your constituents and for your focus on protecting American businesses and consumers from cyber attacks.

Testimony of Arne Sorenson, President & CEO, Marriott International

**Before the
Senate Committee on Homeland Security & Governmental Affairs
Permanent Subcommittee on Investigations
March 7, 2019**

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, thank you for the opportunity to testify today.

The subject the Subcommittee is tackling – private sector cyber-attacks – is an increasingly urgent one that has hit Marriott International directly with the data security incident that we announced on November 30, 2018. We deeply regret this incident. We are committed to supporting our affected guests and enhancing security measures to protect against future attacks.

For 91 years, Marriott has been in the business of serving people. We began as a small family business in Washington, D.C., serving hamburgers and root beer as The Hot Shoppes. Today we are a global hospitality company, conducting operations in all 50 of the United States and 130 countries and territories. Throughout that time, we have built our reputation by putting people first and focusing on the care of our guests.

As a company that prides itself on taking care of people, we recognize the gravity of this criminal attack on the Starwood Guest Reservation Database and our responsibility for protecting our guests' data. To our guests, including our employees who have stayed at Starwood hotels, I sincerely apologize. We are working hard every day to rebuild your confidence.

I. Timeline of Events

In order to explain our current understanding of the incident, it is helpful to start with a chronology of events. Because this incident involved the Starwood Guest Reservation Database,

I will begin with the merger of Marriott and Starwood Hotels & Resorts Worldwide in September 2016.

A. Merger with Starwood

On November 15, 2015, Marriott signed a merger agreement with Starwood, which was announced publicly the following day. The transaction closed on September 23, 2016. During the intervening ten months, we obtained information about Starwood's technology and network and assessed how to integrate the two systems, although our inquiry was legally and practically limited by the fact that, until the merger closed, Starwood remained a direct competitor of Marriott.

Following this evaluation, we made the decision to retain Marriott's reservation system as the central system for the combined group of hotels and to retire Starwood's reservation system. Migrating all of Starwood's 1,270 hotels onto Marriott's reservation system while avoiding disruption of the reservation process for guests and hotels was a significant undertaking over a period of two years. After the close of the merger, we continued to operate the Starwood system and we invested in additional information security measures for that system. In November 2018, we accelerated the timeline to retire the system and, as of December 18, 2018, we are no longer using the Starwood Guest Reservation Database to conduct business operations.

B. Discovery and Investigation of the Incident

On September 8, 2018, Accenture, which managed the Starwood Guest Reservation Database, contacted Marriott's IT team with information about a Guardium alert generated on September 7. Guardium is an IBM security product used on the Starwood system to help secure databases. The Guardium alert was triggered by a query from an administrator's account to return the count of rows from a table in the database. Such a query would not return the content of these rows, only the total number of rows in the table.

As part of our investigation into the alert, we learned that the individual whose credentials were used had not actually made the query. We implemented containment and access control measures, and continued to do so throughout the investigation that followed.

We quickly engaged legal counsel and industry experts to investigate the scale and scope of the incident. On September 10, 2018, two days after Accenture elevated the alert, Marriott brought in third-party investigators to conduct a full investigation into the circumstances that led to the alert and to assist with containment measures. On September 17, 2018, the investigators uncovered a Remote Access Trojan (“RAT”), a form of malware that allows an attacker to covertly access, surveil, and even gain control over a computer. I was notified of the ongoing investigation that day, and our Board was notified the following day.

C. Investigation of the Incident

Uncovering the full scope of the attack took significant forensic work. We worked with and relied on experts in the field to conduct a thorough and careful investigation. In early October 2018, the investigators found on some systems evidence of malware, including MimiKatz, a tool that searches a device’s memory for usernames and passwords. Through the first two weeks of November 2018, although there was evidence of an unauthorized party on the Starwood network since July of 2014, our investigators had found no evidence that the attacker had accessed guest data in the Starwood Guest Reservation Database.

On October 29, 2018, we contacted the FBI to provide them with information about the tools used by the attacker, the timeline of the intrusion, and forensic findings. Since that time, we have provided the FBI with several updates and ready access to forensic findings and information to support their investigation. At the same time, our investigative experts continued their

painstaking forensic work, rolling out endpoint detection technology on devices across the Starwood network.

On November 13, our investigators discovered evidence that two compressed, encrypted files had been deleted from a device that they were examining. The files were encrypted and the actual content was unknown. There was also evidence to suggest that those two files had potentially been removed from the Starwood network. Six days later, on November 19, 2018, investigators were able to decrypt the files, and found that one contained an export of a table from the Starwood Guest Reservation Database containing guest data, while the other contained an export of a table holding passport information.

On November 19, 2018, upon learning that the files the attacker compressed and encrypted contained personal information, we immediately began preparations to notify our guests and regulatory authorities. Recognizing that speed was of the essence, in the days that followed we worked to make sure that we could provide concrete and useful information to our guests. These efforts are described below. While these preparations were ongoing, we also began notifying regulatory authorities.

On November 25 and 26, we found that, in 2015 and 2016, prior to our acquisition of Starwood, the attacker had likely created a copy of two other tables, which the attacker later deleted. The file names correspond to two other tables in the Starwood Guest Reservation Database. We have been unable to recover those files and could not determine if they had been taken.

On November 29, 2018, we gave an update to the FBI and notified the four major payment card networks and their credit card processing vendors. We provided notice to regulators in over

twenty foreign countries and territories, as well as to state Attorneys General, the Federal Trade Commission, the Securities and Exchange Commission, and the three credit reporting agencies.

II. The Scope of the Incident

Our first public announcement about the incident on November 30, 2018 estimated that approximately 500 million guest records were involved, even though we knew that the numbers would likely decrease as our investigation continued and we de-duplicated the records. We issued a follow-up press release on January 4, 2019, adjusting the number of affected records downward to 383 million guest records as a result of our further investigative efforts and certain de-duplication efforts. To be clear, this does not mean that information concerning 383 million unique guests was involved; in many instances, there appear to be multiple records for the same guest, but because of the nature of the data, further de-duplication cannot easily be performed. We cannot confidently determine whether records with similar names, or even identical names with different addresses, represent one person or multiple people, but we have concluded with a fair degree of certainty that information for fewer than 383 million unique guests was involved.

According to our most recent investigative findings, the incident involved approximately 18.5 million encrypted passport numbers and approximately 5.25 million unencrypted passport numbers (approximately 663,000 of which have been associated with the United States). With respect to payment cards, the incident involved approximately 9.1 million encrypted payment card numbers, of which approximately 385,000 were unexpired as of September 2018. Based on our current information, we believe that the information accessed by an unauthorized third party could include several thousand unencrypted payment card numbers. To date, we have not found evidence that the master encryption keys needed to decrypt encrypted payment card and passport numbers were accessed, but we cannot rule out that possibility. Certain data analytics and

investigative work continues, including by a Payment Card Industry Forensic Investigator engaged on behalf of the payment card networks.

III. Marriott Is Dedicated to Providing Support to Guests

We deeply regret that this incident occurred and are focused on responding to our guests' needs and questions. We have therefore created several resources for guests who are concerned that their information may have been involved in the incident.

A. Notification of Guests

While our forensic work was ongoing, Marriott worked to create guest communication documents and coordinate with external vendors to build the logistical infrastructure required to facilitate guest notifications. We wanted to be transparent with our guests and also to be ready on day one to handle inquiries from guests across the world.

On November 30, we provided public notice of the incident via a press release and notification banners across Marriott's websites and the Marriott and Starwood Preferred Guest apps. After the November 30 press release, we also began providing email notifications to various guests who had valid email addresses in the affected tables. We sent email notifications on a rolling basis, and our emails to U.S.-based guests were completed on December 11, 2018.

B. Dedicated Website for Guests

We have created a dedicated website to provide information and updates about the incident and to assist anyone who was potentially affected. The website provides details regarding the incident, the information involved, the steps being taken to investigate, and answers to frequently asked questions (FAQs). The website also has information about how guests can monitor and protect their data and details on both call centers and web monitoring services. The dedicated

website is available in several languages, such as English, Spanish, French, German, Italian, and Portuguese. It can be found at <https://info.starwoodhotels.com>.

C. Call Centers to Answer Guests' Questions

In order to answer guests' questions about the incident, we set up dedicated call centers available in a number of languages, most of which operate seven days per week. We focused on creating call centers that were well staffed so that guests would face minimal wait times. Through February 28, 2019, the average wait time in the United States and Canada is nine seconds. If our call center staff is not able to answer specific questions that a guest may have, there is an escalation process in place to ensure that further efforts are made to respond to inquiries.

Through February 28, 2019, the call centers had received approximately 53,000 calls in total. Significantly, the number of total calls and escalations has been trending steadily downwards, with the exception of a brief increase following the January 4, 2019 press release.

D. Web Monitoring to Help Guests

We are also offering two free monitoring solutions for potentially-affected guests. U.S., U.K., and Canadian guests can enroll in a service called WebWatcher, which monitors the sites where personal information may be shared and alerts guests if evidence of their personal data is found. In the United States, enrollment in WebWatcher provides two additional benefits: fraud loss reimbursement coverage and unlimited fraud consultation services for one year. Through February 28, 2019, approximately 250,750 U.S. guests had activated WebWatcher. In certain other countries, we have engaged Experian to provide its IdentityWorks Global Internet Surveillance product to guests. Through February 28, 2019, approximately 36,000 guests had enrolled in the Experian product.

E. Claims Processing

We have created a process that enables guests or other customers to ask what information about them, if any, was involved in this incident. That process, and an expedited process for ascertaining whether a particular passport number was included in the set of unencrypted passport numbers involved in the incident, can be accessed through a publicly-available link on the dedicated website referenced above. So far, approximately 17,700 requests have been received through this website by guests wanting to know more about whether their information was involved.

Additionally, we have established a process for guests to submit individual claims of fraud related to this incident. We review any claims made by a guest with individual attention, diligence, and care.

F. No Evidence of Fraudulent Use of Information

Thus far, we have not received any substantiated claims of loss from fraud attributable to the incident. Moreover, none of the security firms we engaged to monitor the dark web have found evidence that information contained in the affected tables has been or is being offered for sale. We have not been notified by any banks or card networks that Starwood has been identified as a common point of purchase in any fraudulent transactions, which typically identifies the merchant location where cardholder data was stolen or where a data security breach may have occurred. We will continue to be vigilant for fraudulent use of guest information or attempts by anyone to profit from the incident.

With respect to passport numbers, the State Department has stated that a United States passport number, by itself, cannot be used to travel internationally or procure a new passport.

IV. Marriott Is Improving Security and Privacy Protections Going Forward

As noted above, the Marriott and the Starwood networks have always been separate. This incident affected only the Starwood network. As we combined the Marriott and Starwood organizations after the merger closing, we undertook a review of our systems and set in motion a plan to enhance the security of our systems to address the ever-increasing sophistication of cyber-attackers. As of December 18, 2018, we are no longer using the Starwood Guest Reservation Database for business operations. In the time between the discovery of this incident and the retirement of the Starwood database, we took additional steps to secure the Starwood network, including malware removal, deployment of endpoint protection tools to approximately 70,000 devices that were originally on the Starwood network, rebuilding impacted hosts, and IP whitelisting to control access to the Starwood database.

I want to emphasize that our work here is not limited to payment card industry (PCI) compliance. We had already increased our investment in enhancing our information security prior to the incident, and the incident has caused us to accelerate those efforts and to further increase our investment and speed up planned enhancements. Beyond the steps taken to secure the Starwood network and the retirement of the Starwood Guest Reservation Database, we have accelerated our roll-out of endpoint protection tools to over 200,000 devices. Those tools allow real-time discovery of suspicious behavior on both the Starwood and Marriott networks and have next-generation anti-virus features. We are focused on identity access management, which means a broader deployment of two-factor authentication across our systems, as well as network segmentation, which means isolating the most valuable data so that it becomes more difficult for attackers to access the systems and for malware to spread through the environment.

We are working to identify ways that we can be an industry leader on these issues. We know that this is a race that has no finish line. Cyber-attacks are a pervasive threat. At Marriott, we are committed to taking care of our guests and to proactively finding ways to protect against, detect, and respond to these evolving cyber threats.

I thank the Subcommittee again for the opportunity to testify today.

**PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION
Before the
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
Permanent Subcommittee on Investigations
UNITED STATES SENATE
WASHINGTON, DC
MARCH 7, 2019**

I. INTRODUCTION

Chairman Portman, Ranking Member Carper, and members of the Subcommittee, I am Andrew Smith, Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s testimony on data security.

For nearly two decades, the FTC has been the nation’s leading data security enforcement agency. In that role, the Commission has settled or litigated more than 60 law enforcement actions against businesses that allegedly failed to take reasonable precautions to protect consumers’ personal information. The FTC vigorously pursues data security cases in a variety of areas, including against manufacturers of consumer products like smartphones, computers, routers, and connected toys as well as against companies that collect consumers’ most sensitive personal information.

Data security is critically important both to consumers and to businesses. When a failure to reasonably safeguard consumers’ personal information results in a data breach, consumers can suffer fraud and other harm. Moreover, the specter of data breaches not only affects those individual victims; it can engender a loss of consumer trust in companies, products, technologies, or even business sectors—with an adverse impact on consumers and businesses alike. To combat these harms, the Commission has, for nearly two decades, taken a three-pronged approach to data security: law enforcement, policy initiatives, and consumer and business education. The FTC has also coordinated efforts and resources in this area with other government actors, including the Department of Justice, criminal investigative agencies, and state Attorneys General.

¹ This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

Today, the Commission reiterates its longstanding bipartisan call for enactment of a comprehensive federal data security law. This testimony provides an overview of the Commission's efforts to promote data security, and explains further the Commission's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

Although it does not enforce a comprehensive data security law, the Commission does enforce a number of statutes related to data security. First, it enforces statutes and rules that pertain to specific types of entities and covered data. For example, the Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), requires non-bank financial institutions to safeguard nonpublic personal information by developing, implementing, and maintaining a comprehensive information security program..² The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to verify that recipients of sensitive consumer information act with a permissible purpose,³ and requires entities that maintain consumer report information to use safe disposal procedures.⁴ Finally, the Commission enforces the Children's Online Privacy Protection Act ("COPPA"), which requires website operators to use reasonable security for the personal information they collect from children online.⁵

² 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

³ 15 U.S.C. § 1681e.

⁴ *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

⁵ 15 U.S.C. §§ 6501-6506. The FTC's implementing rule is at 16 C.F.R. Part 312. As part of its vigorous enforcement of COPPA, the FTC announced last week that video social networking app Musical.ly (now known as TikTok) has agreed to pay a record \$5.7 million civil penalty to settle allegations that it illegally collected personal information from children. Press Release, FTC, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That It Violated Children's Privacy Law* (Feb. 27, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc>.

Second, the Commission enforces Section 5 of the FTC Act, which prohibits unfair or deceptive practices.⁶ Although not a data security statute *per se*, the FTC Act empowers the Commission to stop companies from making misleading statements or omissions about data security, where such material statements or omissions are likely to mislead reasonable consumers.⁷ Indeed, the Commission has settled more than 30 matters challenging companies' express and implied claims that they provide reasonable security for consumers' personal data when they allegedly failed to use readily available, cost-effective measures to reduce data security risks.⁸ And the Commission is currently litigating a case in federal district court against a device manufacturer that allegedly deceived consumers about the security of its routers and internet cameras.

The Commission has similarly used the FTC Act's prohibition on unfair practices to stop unreasonable data security practices. Under the statute, if a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices are "unfair."⁹ The Commission has settled over 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.¹⁰

As described above, the Commission has used its authority under these laws to litigate or settle more than 60 data security cases. In each of these instances, the security failures were not merely isolated mistakes. Indeed, the Commission has made clear that it does not require perfect security. There is no one-size-fits-all data security program, and the fact of a breach does not

⁶ 15 U.S.C. § 45(a).

⁷ See Federal Trade Commission Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

⁸ See FTC, Cases Tagged with Data Security, <https://www.ftc.gov/enforcement/cases-proceedings/terms/249> (last visited Feb. 14, 2019).

⁹ See Federal Trade Commission Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984); 15 U.S.C. § 5(n).

¹⁰ See *supra* note 8. Some cases have alleged both deception and unfairness.

necessarily mean that a company's security was unreasonable. Rather, reasonable security requires an ongoing process of assessing and addressing risks. When deciding whether to pursue an action, the Commission considers whether a company's data security measures are reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its operations, and the cost of tools available to reduce data security risks.

Several recent cases illustrate this approach. In a revised settlement with Uber Technologies, Inc.,¹¹ the FTC charged that the popular ride-sharing company deceived consumers by failing to reasonably secure sensitive consumer data stored in the cloud, despite promises of secure storage. Uber's alleged security failures were numerous: using a single key for full administrative access to consumer data, not requiring multi-factor authentication (a widely used, readily available safeguard in this area), and storing sensitive consumer information in plain readable text in database back-ups stored in the cloud. In light of these alleged pervasive, basic security failures, breaches of personal information in 2014 and 2016 were no surprise—and an FTC action to require reasonable security was necessary.

In another case, the FTC settled allegations that mobile phone manufacturer BLU Products, Inc. failed to implement the "appropriate" security procedures it promised.¹² As a result of BLU's security failures, the complaint charged, a third party service provider located in China collected an enormous amount of information from consumers' devices (far more than it needed), including the full contents of consumers' text messages. According to the complaint, had BLU implemented

¹¹ See Press Release, *Federal Trade Commission Gives Final Approval to Settlement with Uber* (Oct. 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber>.

¹² Press Release, *FTC Gives Final Approval to Settlement with Phone Maker BLU* (Sept. 10, 2018), <https://www.ftc.gov/news-events/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu>.

reasonable technical security measures or engaged in reasonable oversight of its service provider, the third party would not have been able to access such sensitive information.

The FTC is currently litigating an action against computer networking equipment manufacturer D-Link, whose alleged inadequate security measures left consumers' wireless routers and internet cameras vulnerable to hackers.¹³ Here, too, the FTC is challenging multiple alleged security failures: shipping software with well-known flaws, mishandling a private code-signing key, and storing login credentials in clear text. This action, like the FTC's other data security cases, sends a clear message: the FTC uses its existing tools to the fullest extent to stop unreasonable data security practices.

B. Policy Initiatives

Law enforcement is not the Commission's only tool; the FTC also uses policy initiatives, such as workshops, reports, and rulemaking, to promote data security. For example, in October 2018, the Commission's legal and economic staff issued their perspective on the FTC's December 2017 Informational Injury Workshop, which explored the injuries consumers may suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.¹⁴ The staff perspective was the second security-related report that the FTC issued in 2018. A report issued earlier in the year, *Mobile Security Updates: Understanding the Issues*, provided in-depth analysis of mobile security update data submitted by eight mobile device manufacturers in response to Commission orders.¹⁵ The report's policy recommendations were grounded in that empirical work.

¹³ Press Release, *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras* (Jan. 5, 2017), <https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate>.

¹⁴ FTC Report, *FTC Informational Injury Workshop: BE and BCP Staff Perspective* (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

¹⁵ FTC Report, *Mobile Security Updates: Understanding the Issues* (Feb. 2018), <https://www.ftc.gov/reports/mobile-security-updates-understanding-issues>.

In November, the FTC held a hearing on data security as part of its series of *Hearings on Competition and Consumer Protection in the 21st Century*.¹⁶ Participants included academics, industry representatives, practitioners, and consumer advocates who discussed a variety of data security-related topics, including the prevalence and consequences of data breaches, incentives to invest in data security, consumer demand for security, data security assessments, and whether the FTC's current toolkit is sufficient to address data security harms.¹⁷ This hearing, like the others in the series, has yielded important information about business and technological changes that affect pressing consumer protection issues.

C. Business Guidance and Consumer Education

The Commission also creates extensive business and consumer education on data security. A recent focus has been cybersecurity guidance for small businesses. In April 2018, the FTC issued *Engage, Connect, Protect*, a staff perspective on the agency's projects and plans in this area.¹⁸ As part of this initiative, the FTC has issued a variety of cybersecurity guidance for small businesses, such as fact sheets, videos, and other materials on dozens of cybersecurity topics.¹⁹ For

¹⁶ See Press Release, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its>.

¹⁷ *FTC Hearing on Competition and Consumer Protection in the 21st Century* – December 2018, <https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018> (last visited Feb. 20, 2019).

¹⁸ FTC Staff Perspective, *Engage, Connect, Protect: The FTC's Projects and Plans to Foster Small Business Cybersecurity* (Apr. 2018), https://www.ftc.gov/system/files/documents/reports/engage-connect-protect-ftcs-projects-plans-foster-small-business-cybersecurity-federal-trade/ecp_staffperspective_2.pdf.

¹⁹ See FTC, *Protecting Small Businesses*, <https://www.ftc.gov/tips-advice/business-center/small-businesses> (last visited Feb. 14, 2019); see also Press Release, *FTC Launches National Campaign with Resources to Assist Small Businesses with Cybersecurity* (Oct. 18, 2018), <https://www.ftc.gov/news-events/press-releases/2018/10/ftc-launches-national-campaign-resources-assist-small-businesses>.

example, recent business guides have covered topics such as email authentication,²⁰ vendor security,²¹ and tech support scams.²²

This guidance builds on the success of the 2017 business education series *Stick with Security*,²³ which offers advice on key security principles based in part on the FTC's closed investigations. The *Stick with Security* series itself expands on *Start with Security*, an earlier Commission initiative on data security that includes a written guide for businesses²⁴ and 11 short videos²⁵ that discuss ten important security topics and give advice about specific security practices for each. The advice in the guide and videos is drawn directly from lessons learned in FTC cases.

The Commission also educates consumers on data security in a variety of ways, such as through its website, videos, and pamphlets. For example, the FTC website highlights timely security issues, like tax identity theft, a Netflix phishing scam, tips on buying internet-connected smart toys, and the aftermath of the Marriott data breach.²⁶ At times, the FTC provides in-depth materials on a data security topic of particular concern to consumers. For example, immediately following the Equifax data breach, the agency created a dedicated page on its website, with information about fraud alerts, active duty alerts, credit freezes and locks, credit monitoring, and how to reduce the risk of identity theft.²⁷ Finally, the FTC assists consumers affected by data breaches through [identitytheft.gov](https://www.identitytheft.gov), a website that allows victims of data breaches to get

²⁰ FTC Business Blog, *Cybersecurity for small business: Email authentication* (Feb. 8, 2019),

<https://www.ftc.gov/news-events/blogs/business-blog/2019/02/cybersecurity-small-business-email-authentication>.

²¹ FTC Business Blog, *Cybersecurity for small business: Vendor security* (Dec. 21, 2018), <https://www.ftc.gov/news-events/blogs/business-blog/2018/12/cybersecurity-small-business-vendor-security>.

²² FTC Business Blog, *Cybersecurity for small business: Tech support scams* (Dec. 14, 2018), <https://www.ftc.gov/news-events/blogs/business-blog/2018/12/cybersecurity-small-business-tech-support-scams>.

²³ FTC, *Stick with Security: A Business Blog Series* (2017), <https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series>.

²⁴ FTC, *Start with Security: A Guide for Business* (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

²⁵ FTC Videos, *Start with Security* (2015-2016), <https://www.ftc.gov/news-events/audio-video/business>.

²⁶ See generally FTC Consumer Blog, <https://www.consumer.ftc.gov/blog> (last visited Feb. 14, 2019).

²⁷ FTC, *The Equifax Data Breach*, <https://www.ftc.gov/equifax-data-breach> (last visited Feb. 14, 2019).

information on how to protect their personal information, and enables identity theft victims to easily file a complaint with the FTC and get a personalized Identity Theft report that can be used to help communicate with financial companies and credit reporting agencies. For victims of tax identity theft, identitytheft.gov helps people file the IRS Identity Theft Affidavit with the IRS – the first-ever digital pathway to do so.

III. DATA SECURITY LEGISLATION

While the Commission uses its existing authorities aggressively, the FTC reiterates its longstanding bipartisan call for comprehensive data security legislation. In particular, the FTC supports data security legislation that would provide the agency with three essential additional authorities: (1) the ability to seek civil penalties to effectively deter unlawful conduct, (2) jurisdiction over non-profits and common carriers, and (3) the authority to issue implementing rules under the Administrative Procedure Act (“APA”), as appropriate.²⁸

Each of these additional authorities is important to the Commission’s efforts to combat unreasonable security. Under current laws, the FTC only has the authority to seek civil penalties for data security violations related to children’s online information (under COPPA) or credit report information (under the FCRA).²⁹ When the FTC brings data security cases under the FTC Act or the GLB Safeguards Rule, it cannot obtain civil penalties for first-time violations. To help ensure effective deterrence, we urge Congress to enact security-specific legislation to allow the FTC to seek civil penalties for data security violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits and common carriers is important because these entities often collect sensitive consumer information. For example, educational institutions often collect

²⁸ While today’s hearing focuses on data security, the Commission recognizes that many aspects of data security intersect with broader questions about consumer data privacy. The Commission urges Congress to consider enacting privacy legislation that would be enforced by the FTC.

²⁹ The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(f).

Social Security numbers and common carriers often collect the contents of consumer communications. Significant breaches have been reported in each of these sectors.³⁰

Finally, the ability to engage in targeted APA rulemaking authority would enable legal requirements to keep up with business and technological changes. For example, in 2012, the FTC used its APA rulemaking authority under COPPA to update its implementing Rule (after giving notice and seeking public comment) to account for the rise of social media and the collection of geolocation information—practices that developed after Congress passed COPPA in 1998.³¹

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumers and data, and we look forward to working with the Subcommittee as it considers these important issues.

³⁰ See, e.g., Andy Segegin, *Hacked! Crooks are Grabbing Nonprofit Websites and Demanding Ransom*, THE NONPROFIT TIMES (Mar. 30, 2017), <http://www.thenonprofittimes.com/news-articles/hacked-crooks-grabbing-nonprofit-websites-demanding-ransom/>; *Spanish Telecom Provider Suffers Massive Data Breach*, SECURITY NEWSPAPER (July 19, 2018), <https://www.securitynewspaper.com/2018/07/19/spanish-telecom-provider-suffers-massive-data-breach/>.

³¹ Press Release, *FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule* (Dec. 19, 2012) <https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over>.

United States Government Accountability Office



Testimony

Before the Permanent Subcommittee on
Investigations, Committee on Homeland
Security and Governmental Affairs, U.S.
Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, March 7, 2019

INTERNET PRIVACY AND DATA SECURITY

Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility

Statement of Alicia Puente Cackley, Director, Financial
Markets and Community Investment

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee:

Thank you for the opportunity to testify today about Internet privacy and data security issues. The United States does not have a comprehensive data privacy law at the federal level and instead relies in part on a sectoral approach with industry-specific laws enforced by various agencies governing areas such as healthcare and financial services. In addition, the Federal Trade Commission (FTC) currently has the lead in overseeing Internet privacy across all industries, with some exceptions. Specifically, FTC addresses consumer concerns about Internet privacy using its broad authority to protect consumers from unfair and deceptive trade practices. FTC has jurisdiction over a broad range of entities and activities that are part of the Internet economy, including websites, applications (apps), advertising networks, data brokers, device manufacturers, and others.

My testimony today addresses (1) FTC's role and authorities for overseeing Internet privacy, (2) stakeholders' views on potential actions to enhance federal oversight of consumers' Internet privacy, and (3) breaches of personally identifiable information. This statement is primarily based on our January 2019 report on Internet privacy.¹ This work included evaluating FTC's Internet privacy enforcement actions and authorities and interviewing various stakeholders, including representatives from industry, consumer advocacy groups, and academia, as well as FTC staff and former FTC and Federal Communications Commission (FCC) commissioners. We also interviewed officials from other federal oversight agencies—such as the Consumer Financial Protection Bureau (CFPB), Food and Drug Administration (FDA), and the Equal Employment Opportunity Commission (EEOC)—about the strengths and limitations of their regulatory and enforcement authorities and approaches. A complete description of our scope and methodology can be found in our January 2019 report. This statement also includes some additional information on data breaches from our August 2018 report on Equifax.²

¹GAO, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GAO-19-52 (Washington, D.C.: Jan. 15, 2019).

²GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, GAO-18-559 (Washington, D.C.: Aug. 30, 2018).

We conducted the performance audit on which this statement is primarily based from October 2017 through January 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In April 2018, Facebook disclosed that a Cambridge University researcher may have improperly shared the data of up to 87 million of Facebook's users with a political consulting firm. This followed other incidents in recent years involving the misuse of consumers' personal information from the Internet, which about three-quarters of Americans use. These types of incidents have raised public concern because Internet-based services and products, which are essential for everyday social and economic purposes, often collect and use various forms of personal information that could cause users harm if released.

The federal privacy framework for private-sector companies is comprised of a set of tailored laws that govern the use and protection of personal information for specific purposes, in certain situations, or by certain sectors or types of entities. Such laws protect consumers' personal information related to their eligibility for credit, financial transactions, and personal health, among other areas.³

We reported in 2013 that no overarching federal privacy law governs the collection and sale of personal information among private-sector companies, including information resellers—companies that collect and resell information on individuals.⁴ We found that gaps exist in the federal privacy framework, which does not fully address changes in technology and the marketplace. We recommended that Congress consider legislation to strengthen the consumer privacy framework to reflect the effects of changes in technology and the marketplace. Such legislation has not been enacted.

³These laws include the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act.

⁴GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

FTC's Role and Authorities for Overseeing Internet Privacy

As we reported in January 2019, FTC is primarily a law enforcement agency with authority to, among other things, address consumer concerns about Internet privacy, both for Internet service providers and content providers. It does so using its general authority under section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."⁵

Even though the FTC Act does not speak in explicit terms about protecting consumer privacy, the Act authorizes such protection to the extent it involves practices FTC defines as unfair or deceptive. According to FTC, an act or practice is "unfair" if it causes, or is likely to cause, substantial injury not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition as a result of the practice. FTC has used this "unfairness" authority to address situations where a company has allegedly failed to properly protect consumers' data, for example. According to FTC, a representation or omission is "deceptive" if it is material and is likely to mislead consumers acting reasonably under the circumstances. FTC has applied this "deceptiveness" authority to address deceptions related to violations of written privacy policies and representations concerning data security, for example.

FTC staff investigate Internet privacy complaints from various sources and also initiate investigations on their own. If FTC staff have reason to believe that an entity is engaging in an unfair or deceptive practice, they may forward an enforcement recommendation to the commission. The commission then determines whether to pursue an enforcement action.⁶ With certain exceptions, FTC generally cannot directly impose civil monetary penalties for Internet privacy cases. Instead, FTC typically addresses Internet privacy cases by entering into settlement agreements requiring companies to take actions such as implementing reasonable privacy and security programs. If a company then violates its settlement agreement with FTC, the agency can request civil monetary penalties in court for the violations. In addition, FTC can seek to impose civil monetary penalties directly for violations of certain statutes and their

⁵15 U.S.C. § 45(a)(1).

⁶FTC staff operate separately from the FTC commission itself, which is the set of five commissioners, including the chair, who ultimately have responsibility for deciding upon courses of action, including enforcement actions.

implementing regulations, such as the statute pertaining to the Internet privacy of children and its corresponding regulations.

FTC has not promulgated rules under section 5 specific to Internet privacy. According to FTC staff, the process the agency must use to issue such rules—known as the Magnuson-Moss procedures—includes steps that add time and complexity to the rulemaking process. FTC has not promulgated any regulations using the Magnuson-Moss procedures since 1980. Although FTC has not implemented its section 5 authority by issuing regulations regarding internet privacy, it has issued regulations when directed and authorized by Congress to implement other statutory authorities using a different set of rulemaking procedures. These procedures, spelled out in section 553 of the Administrative Procedures Act (APA),⁷ are those that most federal agencies typically use to develop and issue regulations.

APA section 553 establishes procedures and requirements for what is known as “informal” rulemaking, also known as notice-and-comment rulemaking. Among other things, section 553 generally requires agencies to publish a notice of proposed rulemaking in the *Federal Register*. After giving interested persons an opportunity to comment on the proposal by providing “data, views, or arguments,” the statute then requires the agency to publish the final rule in the *Federal Register*.

In contrast, the rulemaking procedures that FTC generally must follow to issue rules under the FTC Act are the Magnuson-Moss procedures noted above. These are required by the Magnuson-Moss Warranty Act amendments to the FTC Act and impose additional rulemaking steps beyond APA section 553. These steps include providing the public and certain congressional committees with an advance notice of proposed rulemaking (in addition to the notice of proposed rulemaking). FTC’s rulemaking under Magnuson-Moss also calls for, among other things, oral hearings, if requested, presided over by an independent hearing officer, and preparation of a staff report after the conclusion of public hearings, giving the public the opportunity to comment on the report.

FTC has promulgated regulations using the APA section 553 notice-and-comment rulemaking procedures when authorized or directed by specific statutes. For example, the 1998 Children’s Online Privacy Protection Act

⁷5 U.S.C. § 553.

(COPPA) required FTC to issue regulations concerning children's online privacy; promulgate these regulations using the APA section 553 process; and, in determining how to treat a violation of the rules, to treat it as an unfair or deceptive act or practice in most cases. COPPA governs the online collection of personal information from children under the age of 13 by operators of websites or online services, including mobile applications. COPPA contained a number of specific requirements that FTC was directed to implement by regulation, such as requiring websites to post a complete privacy policy, to notify parents directly about their information collection practices, and to obtain verifiable parental consent before collecting personal information from their children or sharing it with others.

Laws and regulations may be enforced in various ways, for example, by seeking civil monetary penalties for non-compliance. As mentioned, FTC has authority to seek civil monetary penalties when a company violates a settlement agreement or certain statutes or regulations. For example, in March 2018, FTC announced that it is investigating whether Facebook's current privacy practices violate a settlement agreement that the company entered into with FTC. In the case that resulted in the 2012 settlement, FTC had charged Facebook with deceiving consumers by telling them they could keep their information private, but then allowing it to be shared and made public. FTC also has authority to seek civil monetary penalties for violations of the COPPA statute as well as FTC's COPPA regulations.

In our January 2019 Internet privacy report, we found that during the last decade, FTC filed 101 Internet privacy enforcement actions to address practices that the agency alleged were unfair, deceptive, a violation of COPPA, a violation of a settlement agreement, or a combination of those reasons. Most of these actions pertained to first-time violations of the FTC Act for which FTC does not have authority to levy civil monetary penalties. In nearly all 101 cases, companies settled with FTC, which required the companies to make changes in their policies or practices as part of the settlement.

**Stakeholders and
FTC Identified
Potential Actions to
Enhance Federal
Oversight of
Consumers' Internet
Privacy**

Various stakeholders we interviewed for our January 2019 Internet privacy report said that opportunities exist for enhancing Internet privacy oversight. Most industry stakeholders said they favored FTC's current approach—direct enforcement of its unfair and deceptive practices statutory authority, rather than promulgating and enforcing regulations implementing that authority. These stakeholders said that the current approach allows for flexibility; that regulations could hinder innovation, create loopholes, and become obsolete; and that rulemakings can be lengthy. Other stakeholders, including consumer advocates and most former FTC and FCC commissioners we interviewed, favored having FTC issue and enforce regulations. Stakeholders said that regulations can provide clarity, flexibility, and act as a deterrent, and may also promote fairness by giving companies notice of what actions are prohibited.

Those stakeholders who believe that FTC's current authority and enforcement approach is unduly limited identified three main actions that could better protect Internet privacy: (1) enactment of an overarching federal privacy statute to establish general requirements governing Internet privacy practices of all sectors, (2) APA section 553 notice-and-comment rulemaking authority, and (3) civil penalty authority for any violation of a statutory or regulatory requirement, rather than allowing penalties only for violations of settlement agreements or consent decrees that themselves seek redress for a previous statutory or regulatory violation.

Privacy Statute

Stakeholders from a variety of perspectives—including academia, industry, consumer advocacy groups, and former FTC and FCC commissioners—told us that a statute could enhance Internet privacy oversight by, for example, clearly articulating to consumers, industry, and privacy enforcers what behaviors are prohibited. Some stakeholders suggested that such a framework could either designate an existing agency (such as FTC) as responsible for privacy oversight or create a new agency. For example, in Canada, the Office of the Privacy Commissioner, an independent body that reports directly to the Parliament, was established to protect and promote individuals' privacy rights.

Some stakeholders also stated that the absence of a comprehensive Internet privacy statute affects FTC's enforcement. For example, a former federal enforcement official from another oversight agency said that FTC is limited in how it can use its authority to take action against companies' unfair and deceptive trade practices for problematic Internet privacy practices. Similarly, another former federal enforcement official from

another agency said that FTC is limited in how and against whom it can use its unfair and deceptive practices authority noting, for example, that it cannot pursue Internet privacy enforcement against exempted industries.⁸

In addition, some stakeholders said FTC's section 5 unfair and deceptive practices authority may not enable it to fully protect consumers' Internet privacy because it can be difficult for FTC to establish that Internet privacy practices are legally unfair. Because of this difficulty, some stakeholders said that FTC relies more heavily on its authority to take enforcement action against deceptive trade practices compared with the agency's unfair trade practices authority. This is consistent with the results of our analysis of FTC cases, which showed that in a majority of the actions FTC settled, FTC alleged that companies engaged in practices that were deceptive. Furthermore, a recently decided federal appeals court case illustrates potential limits on FTC's enforcement remedies. The court found that FTC could not direct the company, which was accused of unfair practices, to create and implement comprehensive data security measures for the personal information the company stored on its computer networks as a remedy for the practices alleged. Instead, the court ruled that FTC's authority was limited to prohibiting specific illegal practices.⁹

APA Notice-and-Comment
Rulemaking

Various stakeholders said that there are advantages to overseeing Internet privacy with a statute that provides APA section 553 notice-and-comment rulemaking authority. Officials from other consumer and worker protection agencies we interviewed described their enforcement authorities and approaches. For example, officials from CFPB and FDA, both of which use APA section 553 notice-and-comment rulemaking, said that their rulemaking authority assists in their oversight approaches and supports their enforcement actions. EEOC officials said that regulations are used to guide investigations that establish whether enforcement action is appropriate.

⁸The FTC Act prohibits FTC from taking action against companies such as telecommunications carriers, airlines and railroads under certain circumstances. FTC also does not have jurisdiction over banks, credit unions, or savings and loans institutions.

⁹In this case, FTC filed a complaint against LabMD, a medical laboratory, under section 5 of the FTC Act for allegedly committing an unfair act or practice by failing to provide reasonable and appropriate security for personal information on its computer networks. On appeal, the Eleventh Circuit ruled that FTC's cease and desist order exceeded its authority because it did not prohibit a specific act or practice but instead, mandated a complete overhaul of the company's data-security program. *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018).

Ability to Levy Civil Penalties for Initial Violations

Some stakeholders suggested that FTC's ability to levy civil penalties could also be enhanced. As noted, FTC can levy civil penalties against companies for violating certain regulations, such as COPPA regulations, or for violating the terms of a settlement agreement already in place. According to most former FTC commissioners and some other stakeholders we interviewed, FTC should be able to levy fines for initial violations of section 5 of the FTC Act. An academic told us that the power of an agency to levy a fine is a tangible way to hold industries accountable.

Breaches Involving Personally Identifiable Information Highlight the Importance of Security and Privacy

Recent data breaches at federal agencies, retailers, hospitals, insurance companies, consumer reporting agencies, and other large organizations highlight the importance of ensuring the security and privacy of personally identifiable information collected and maintained by those entities. Such breaches have resulted in the potential compromise of millions of Americans' personally identifiable information, which could lead to identity theft and other serious consequences. For example, the breach of an Equifax online dispute portal from May to July 2017 resulted in the compromise of records containing the personally identifiable information of at least 145.5 million consumers in the United States and nearly 1 million consumers outside the United States. We reported in August 2018 that Equifax's investigation of the breach identified four major factors—identification, detection, segmenting of access to databases, and data governance—that allowed the attacker to gain access to its network and extract information from databases containing personally identifiable information.¹⁰ In September 2017, FTC and CFPB, which both have regulatory and enforcement authority over consumer reporting agencies such as Equifax, initiated an investigation into the breach and Equifax's response. Their investigation is ongoing.

According to a 2017 National Telecommunications and Information Administration (NTIA) survey conducted by the U.S. Census Bureau, 24 percent of American households surveyed avoided making financial transactions on the Internet due to privacy or security concerns.¹¹ NTIA's survey results show that privacy concerns may lead to lower levels of economic productivity if people decline to make financial transactions on

¹⁰GAO-18-559.

¹¹NTIA, *Most Americans Continue to Have Privacy and Security Concerns*, NTIA Survey Finds (Washington, D.C.: Aug. 20, 2018) available at <https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds> (last visited Mar. 5, 2019).

the Internet. Consumers who were surveyed indicated that their specific concerns were identity theft, credit card or banking fraud, data collection by online services, loss of control over personal information, data collection by government, and threats to personal safety.

Recent data breaches and developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider what additional actions are needed to protect consumer privacy, including comprehensive Internet privacy legislation. Although FTC has been addressing Internet privacy through its unfair and deceptive practices authority and FTC and other agencies have been addressing this issue using statutes that target specific industries or consumer segments, the lack of a comprehensive federal privacy statute leaves consumers' privacy at risk. Comprehensive legislation addressing Internet privacy that establishes specific standards and includes APA notice-and-comment rulemaking and first-time violation civil penalty authorities could enhance the federal government's ability to protect consumer privacy, provide more certainty in the marketplace as companies innovate and develop new products using consumer data, and provide better assurance to consumers that their privacy will be protected. In our January 2019 report, we recommended that Congress consider developing comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving Internet environment. Issues that should be considered include:

- which agency or agencies should oversee Internet privacy;
- what authorities an agency or agencies should have to oversee Internet privacy, including notice-and-comment rulemaking authority and first-time violation civil penalty authority; and
- how to balance consumers' need for Internet privacy with industry's ability to provide services and innovate.

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

**GAO Contact and
Staff
Acknowledgments**

For further information regarding this testimony, please contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov or Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Individuals who made key contributions to this testimony include Andrew Huddleston, Assistant Director; Kay Kuhlman, Assistant Director; Bob Homan, Analyst-in-Charge; Melissa Bodeau; John de Ferrari; Camilo Flores; Nick Marinos, and Sean Standley.



31 Tech Valley Drive
 East Greenbush, NY 12061 USA
 518.266.3460
www.cisecurity.org

**Testimony of John Gilligan
 Chief Executive Officer
 Center for Internet Security
 Hearing on Private Sector Data Breaches
 Permanent Subcommittee on Investigations
 Homeland Security & Government Affairs Committee
 United States Senate
 106 Dirksen Senate Office Building
 Washington, DC
 Thursday, March 7, 2019
 10:00 a.m. ET**

Chairman Portman, Ranking Member Carper, and members of the Subcommittee, thank you for inviting me today to this hearing. My name is John Gilligan, and I serve as the Chief Executive Officer of the nonprofit Center for Internet Security, Inc. (CIS). I have spent most of my career in service to the Federal government, including serving as the Chief Information Officer of both the U.S. Department of Energy, and the U.S. Air Force. I appreciate the opportunity today to share our thoughts on the current state of national cybersecurity, focusing on an area we know well: cyber defense. I look forward to offering our ideas on how we can collectively build on the progress being made in this important area of critical national security.

In short, we will: (1) introduce you to CIS and the Critical Security Controls; (2) identify general trends and root causes of recent cyber-attacks; and (3) explain how the CIS Critical Security Controls can help private—and public—sector organizations implement what we call “effective cyber defense”. I will close with some recommendations.

About CIS and the CIS Critical Security Controls

Established in 2000 as a nonprofit organization, the Center for Internet Security’s (CIS’) primary mission is to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for security hardening of commercial IT systems at a time when there was little online security leadership. Today, CIS works with the global security community using collaborative deliberation processes to define security best practices for use by government and private-sector entities. The approximately 200 professionals at CIS provide cyber expertise in three main program areas: (1) the Multi-State and more recently the Elections Infrastructure Information Sharing and Analysis Center, the MS-ISAC and EI-ISAC respectively; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.



MS-ISAC¹. In 2010, the U.S. Department of Homeland Security (DHS), under the then-National Protection and Programs Directorate (NPPD), partnered with CIS to host the MS-ISAC, which has been designated by DHS as the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments as well as all 79 Fusion Centers nationwide. MS-ISAC members include all 56 states and territories and more than 5,000 other SLTT government entities. MS-ISAC's 24x7 cybersecurity operations center provides: (1) cyber threat intelligence that enables MS-ISAC members to gain situational awareness and prevent incidents, consolidating and sharing threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC); (2) early warning notifications containing specific incident and malware information that might affect them or their employees; (3) incident response support; and (4) various educational programs and other services. Furthermore, MS-ISAC provides around-the-clock network monitoring services with our so-called 'Albert' network monitoring devices for many SLTT networks, analyzing over one (1) trillion event logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS-ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. In 2018, MS-ISAC analyzed, assessed, and reported on over 56,000 instances of malicious activity to over 4,000 MS-ISAC members.

EI-ISAC². In 2018 CIS was tasked by DHS to stand up an information sharing and analysis center focused on the Nation's elections infrastructure. Leveraging the experience gained through the MS-ISAC, CIS established the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC is now fully operational with all 50 states participating and over 1500 total members, including elections vendors. The EI-ISAC provides elections officials and their technical teams with regular updates on cyber threats, cyber event analysis, and cyber education materials. During the 2018 primaries and mid-term elections the EI-ISAC hosted the National Cyber Situational Awareness Room, an on-line collaboration forum to keep elections officials aware of cyber and non-cyber incidents and potential cyber threats. More than 600 elections officials participated in these forums. Moreover, CIS was processing data from 135 Albert sensors monitoring the networks, which supported on-line elections functions such as voter registration and election night reporting. The Albert sensors processed 10 petabytes of data during 2018, resulting in over three thousand actionable notifications to elections offices.

CIS Benchmarks. CIS is also the world's largest producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Security Benchmarks (also known as "configuration guides" or "security checklists") provide highly detailed security setting recommendations for a large number of commercial IT products, such as operating systems, data base products and networking systems. These benchmarks are vital for any credible security program. The CIS Security Benchmarks are developed through a collaborative effort of public and private sector security experts. Over 200 consensus-based Security Benchmarks have been

¹ : Find out more information about the MS-ISAC here: <https://msisac.cisecurity.org/>. List of MS-ISAC services here: <https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf>

² A list of EI-ISAC services can be found here: <https://www.cisecurity.org/ei-isac/ei-isac-services/>



developed and are available in PDF format free to the general public on the CIS or NIST web sites. An automated benchmark format along with associated tools is also available through the purchase of a membership. CIS has also created a number of security configured cloud environments, called 'hardened images' that are based on the benchmarks that we are deploying in the Amazon, Google, and Microsoft cloud environments. These hardened images help ensure that cloud users can have confidence in the security provided within the cloud environment they select. The CIS hardened images are used worldwide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Security Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

- NIST Guide for Security-Focused Configuration Management of Information System
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan
- DHS Continuous Diagnostic Mitigation Program
- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI) (April 2016)
- CIS Critical Security Controls

CIS Controls³. CIS' third program is most applicable to today's hearing topic. In 2015, CIS became the home of the CIS Critical Security Controls, previously known as the SANS Top 20, the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene or essential cyber defense. They are developed by an international consensus process and are available free on the CIS web site. The Critical Security Controls or just the CIS Controls have been assessed as preventing up to 90% of pervasive and dangerous cyber-attacks⁴. The CIS Controls act as a blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order—achieving the goals set out by the NIST Cybersecurity Framework (CSF). Moreover, the CIS Critical Security Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cyber security program⁵.

General Trends and Root Causes of Recent Cyber Attacks

In cybersecurity, there are no silver bullets. We must start with the basics. Fortunately, most methods of attacks are well known, as are basic defenses to these attacks. Basic cyber hygiene remains a critical solution to improving American cyber defenses, and the CIS Controls remain a clear, actionable, and free blueprint to implementation of what we call 'essential cyber defense'. Others use the term 'basic cyber

³ Find out more information about the CIS Controls and download them for free here: <https://www.cisecurity.org/critical-controls.cfm>

⁴ Up to 91% of all security breaches can be auto-detected when release, change and configuration management controls are implemented. IT Process Institute: <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533052750.pdf>

⁵ **NIST Framework**, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC"—Council on Cyber Security (the predecessor organization to CIS for managing the Controls) Critical Security Controls)



hygiene'. As noted above, deploying the top five CIS Critical Security Controls can reduce up to 90 percent of known pervasive and dangerous cyber-attacks.⁶

It is also important to note that good information technology (IT) operations (systems and network management) go hand-in-hand with good security. The foundation of good security is good IT management: knowing what you have, how it is configured, when things change, and what can change or bypass security settings. Security considerations begin with your IT operations infrastructure, not a separate security infrastructure. As CIO of the Air Force, I found that by implementing benchmark compatible operating system configurations and tools to ensure that the configurations were not modified resulted in improved security, better operational availability, and reduced costs. The cost reductions were the result of the need for fewer systems and network administrators. The CIO of the State of Arizona has documented similar cost reduction experiences.⁷ The point here is that, contrary to common perception, better security can often cost less rather than better security resulting in increased costs.

Specific Examples of Breach Causes Tracked to the CIS Controls

Overall, 2018 brought the second-highest number of reported data breaches of any year on record. More than 6,500 publicly disclosed breaches and over 5 billion records exposed. We have seen more big data breaches, ransomware, and critical infrastructures hacked.⁸ CIS has analyzed the data for breaches where the root cause has been made public and has found that in each case the root cause related to the failure to properly implement one or more of the CIS Controls. In essence, the root cause of these breaches is the failure to exercise basic cyber hygiene or essential cyber defense. Despite having the concept of the Controls around for a decade, we find that organizations are not implementing the basic hygiene/basic cyber defense.

Many organizations collect and retain large quantities of personally identifiable information (PII) about American citizens or other sensitive data. Any party that handles our PII has the responsibility to do their utmost to protect it. The CIS Controls establish the technical actions that must be implemented to provide basic security. In the Equifax breach, those include:

CIS Control 2: Understand and control what software is running. (And be doubly certain if it is the software that handles or protects sensitive data.)

CIS Control 3: Know what your critical software is and ensure that you have kept up to date on patches. (If there is a known vulnerability, patch it)

CIS Control 6: Audit everything, centralize the audit records, and analyze them. (At a minimum, collect enough data so forensics experts can make full sense of it and help everyone else discover

⁶ <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533052750.pdf>

⁷ <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-does-arizona-government-address-information-security.html>

⁸ <https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report>



and prevent similar attacks.)

CIS Control 9: Limit and control network ports, protocols and services (Operate critical services on separate devices. That makes it easier to see malicious actions. You can see if the attackers exfiltrated data? Did they open ports? Was there a host-based firewall?)

CIS Control 12: Defend the boundaries of your network. (Was traffic to and from the compromised devices being inspected? Did a server initiate an unexpected connection?)

CIS Control 14: Control access based on need to know. (Complexity is the cover used by attackers. Did Equifax segment its network so that critical business functions with user's data could be monitored more closely for anomalies?)

While NotPetya was world-wide in scope [Maersk, Merck, UK National Health System] even a sophisticated attack such as this one consists of numerous individual steps, many of which would have been detected, blocked, or prevented by a series of defensive actions that are found in a subset of the CIS Critical Security Controls. For example, there are CIS Controls that require visibility of all of the hardware and software on the network; removal of outdated, un-securable software; timely patching for known vulnerabilities; and separation of the network into sensitive and less-sensitive areas. There are also CIS Controls to ensure that plans are in place for recovery in case of a security breach. These critical security controls would have prevented, blocked, or managed the effects of the NotPetya attack at multiple cost-effective points.

In the recent Marriott case involving a data breach impacting approximately 500 million customers, a guest registration database from its Starwood properties had been compromised in 2014 — a full two years before Marriott purchased Starwood. Although the specific root causes of the attack have not been made public, based on analysis of other breaches the root causes will likely track to a failure to properly implement one or more of the CIS Controls. *Forbes* recently recommended that a thorough cybersecurity audit should be a part of any company's mergers and acquisitions due diligence process.⁹ Our recommendation is that the CIS Controls be an element in this cyber due diligence process.

Leveraging the CIS Critical Security Controls to Reduce Cyber Attacks

The CIS Controls are especially effective because they are regularly updated by a global network of cyber experts based on actual attack data derived from a variety of public and private threat sources. The Controls help deal with what has sometimes been referred to as “the Fog of More,”—the confusion facing many organizations trying to sort through the many volumes of guidelines and frameworks as well as the constant barrage of marketing from cyber product companies. In essence, the Controls help organizations by cutting through the “fog” by providing a concise set of specific technical actions that track to the common attack patterns so individual organizations do not have to be capable of doing a sophisticated risk

⁹ Forbes, March 1, 2019: <https://www.forbes.com/sites/forbestechcouncil/2019/03/01/do-you-do-security-due-diligence-before-a-merger-or-acquisition/#5ae78a024535>



assessment, the typical starting point of cyber risk frameworks such as the NIST CSF, as well as standards from the Payment Card Industry (PCI), the International Standards Organization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE).

The *California Data Breach Report* (2016)¹⁰, released by then-Attorney General Harris, established the world's first de facto minimum level of information security by warning that failing to implement all relevant Controls "constitutes a lack of reasonable security." Since then, other public organizations have followed California's lead. The State of Ohio also recently established the CIS Controls as the standard for cyber defense within the state.¹¹ The Republic of Paraguay has also mandated compliance with the Controls for government systems.¹² ETSI, the European Standards Organization, has adopted the CIS Controls as its standard for cybersecurity.¹³ The Aerospace Industries Association (AIA) recently published their cybersecurity guidelines, which are based on the CIS Controls.¹⁴ The Atlantic Council has also endorsed the Controls.¹⁵

We are encouraged that many organizations are catching on to the value of the CIS Controls. Security providers have also endorsed the Controls. Symantec, Verizon, and Tripwire have all identified the Controls as being the foundation for effective cyber defense.^{16 17 18}

There is also a need to improve cybersecurity in the Federal government. CIS has been involved with knowledge sharing with the Government Accountability Office on aspects of the cybersecurity of elections infrastructure as well as discussions to improve the evaluation of the state of cybersecurity in the Federal government. We are also involved in discussions regarding the cloud computing policy of the U.S. Department of Defense.¹⁹

Possible Congressional Actions for Helping Prevent Future Cyber Breaches

As the U.S. Congress continues to consider the best ways to improve cybersecurity in the U.S., we respectfully offer our perspectives and our expertise to you as you determine how best to encourage the increased use of basic cyber hygiene and the adoption of voluntary best practices.

We start with the recognition that the NIST's Cybersecurity Framework is an excellent guidance document and serves as the top-level framework for addressing cyber security within the United States.

¹⁰ Report here: <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf> (see Recommendation 1).

¹¹ <https://www.arentfox.com/perspectives/alerts/ohio-passes-first-safe-harbor-law-incentivizing-cybersecurity-controls>

¹² <http://www.cert.gov.py/index.php/guias-de-seguridad> (Google will translate)

¹³ http://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/02.01.01_60/tr_10330501v020101p.pdf

¹⁴ <http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf>

¹⁵ <http://publications.atlanticcouncil.org/cybersecurity/risk-nexus-september-2015-overcome-by-cyber-risks.pdf>

¹⁶ <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>, pages 75-77

¹⁷ Verizon's 2015 Data Breach [Verizon DBIR 2015](#), page 55

¹⁸ <http://www.tripwire.com/state-of-security/featured/20-csc-list-post/>

¹⁹ Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 3, 6 March 2017. (search on 'CIS Benchmarks')



However, by design, the NIST Framework was developed at a general level and within the Framework it points to other, more detailed standards and best practices for specific implementation guidance (including the Critical Security Controls). While a logical construct, this approach has some unintended consequences. In particular, government and private sector organizations who wish to implement the NIST Framework must select for implementation from among very comprehensive lists of standards and best practices that are referenced in the Framework. As noted earlier, this contributes to the “fog of more”—organizations struggling to select the appropriate implementation guidance.

This same problem is magnified for organizations that are required to comply with multiple frameworks. Financial organizations are required to certify against the Payment Card Industry (PCI) framework. Organizations with international presence are often required to follow International Standards Organization (ISO) cybersecurity frameworks. These, and other frameworks have the same unintended consequence as the NIST Cybersecurity Framework. They are excellent high-level guidelines, but lack specificity regarding specifically what security controls should be implemented and in what priority. Working with state and local governments in operating the MS-ISAC, we see the enormous complexity resulting from the requirement to comply with frameworks specified by different Federal, State or domain policies. While the individual policies and regulations are well intended, they are contributing to much confusion and inefficiency in achieving the common goal of basic cyber defense.

Recognizing that our multiple cybersecurity frameworks and duplicative policies have contributed to a real “fog of more” for U.S. organizations, we would recommend that Congress help move the Nation to a solution. Specifically, we recommend that NIST be chartered to develop a single implementation guideline that can be used to satisfy the requirements of the NIST Framework, PCI, ISO, IEEE, and others similar general frameworks. This implementation guideline, we believe, should provide clear guidance on what constitutes cyber hygiene (or essential cyber defense) and recommendations regarding the prioritization of implementation of security controls. We note that the United Kingdom and Australia have done exactly this with the Australian Signals Directorate’s Essential Eight (controls)²⁰ and the United Kingdom National Cyber Security Center’s Cyber Essentials.²¹

CIS recently parsed the Critical Security Controls into three ‘Implementation Groups’ to assist organizations in phasing the implementing the Controls. The Implementation Groups provide a step-by-step path to achieving effective defense against the most common cyber-attack patterns. Implementation Group 1 consists of 43 detailed, technical subcontrols that address the most frequent attacks and are relatively straightforward to implement. We would recommend that Implementation Group 1 or an equivalent be established as the National Cyber Baseline for all organizations who could assess their compliance. In this way, senior leaders in public and private organizations, Congress, and the American public can have an objective basis for measuring the ability of organizations to withstand expected cyber-attacks.

²⁰ <https://acsc.gov.au/infosec/mitigationstrategies.htm>

²¹ <https://www.cyberessentials.ncsc.gov.uk/2017/11/27/a-brief-history-of-cyber-essentials>



Conclusion

We recognize that the cybersecurity problem is a hard one, and one that continues to evolve. However, we also know how to prevent the majority of cyber-attacks. The CIS Critical Security Controls is a proven example of a way to prevent these attacks. We encourage Congress to recognize the current “fog of more” that is inhibiting our progress in implementing effective cyber defense and to require that a technically oriented baseline for cyber defense be established and implemented. We offer the Critical Security Controls as a point of departure or a model for such an effort.

EQUIFAX®**DRAFT**

TO..... [REDACTED] VP, GPS Application Services
 VP, International
 VP Security Engineering Solutions

FROM..... [REDACTED] AVP Technical
 Technical Audit Manager

CC..... [REDACTED] Chief Financial Officer
 SVP Internal Audit
 Chief Information Officer
 Chief Legal Officer
 Chief Security and Privacy Officer
 SVP – Technology
 VP, IT Strategy and Effectiveness

SUBJECT..... Configuration - Patch Management Audit

DATE..... October 28, 2015

Executive Summary

We performed a review of the control procedures related to Configuration, Patch and Vulnerability Management. The purpose of the review was to assess the security of the production networks. [REDACTED]

We noted that current patch and configuration management controls are not adequately designed to ensure Equifax systems are securely configured and patched in a timely manner. As of August 2015, there are over 1000 known critical/high/medium vulnerabilities on externally facing systems (approximately 1150 hosts) and over 7500 critical/high vulnerabilities (not including medium) on internal systems (approximately 22,000 hosts). Of those known vulnerabilities, approximately 75% of the external, and 93% of the internal, vulnerabilities are over 90 days old.

Equifax Confidential and Proprietary

INFORM ► ENRICH ► EMPOWER

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
 CONTAINS SENSITIVE TECHNICAL AND/OR SECURITY RELATED INFORMATION

EFXCONG-PSI000032256

The key issues related to ineffective patch and configuration management are:

- Most Equifax systems are not being patched proactively. Information Security informs IT of security vulnerabilities identified in their monthly scans and then IT is required to patch the system.
- [REDACTED]
- [REDACTED]
- A complete and accurate inventory of Equifax IT assets does not exist. Lack of asset management controls may result in systems not being scanned periodically for vulnerabilities and also does not allow the ability for IT to monitor/manage the patch levels and configuration for all systems.
- There is no consistent process to ensure an adequate risk assessment is performed for identified vulnerabilities to assess the risk to the organization. [REDACTED]

Background

Patch Management: Refers to the process of applying updates to computer assets to address known security vulnerabilities. Vendors produce security patches for their product vulnerabilities and make them available to users. Research has shown that the most efficient way to be protected against attacks is to ensure that every machine in the environment has the latest patches installed. If one computer in the environment is not patched, it can threaten the stability of the entire environment.

Configuration Management: Refers to the process of implementing and maintaining changes to network hardware and software. Many of these configuration settings have a direct impact on the security of that system. To ensure that the required adjustments to the system configuration do not adversely affect the security of the information, a well-defined configuration management process that integrates information security is needed.

Vulnerability Management: This includes the process of identifying, assessing, prioritizing and remediating IT security vulnerabilities to ensure the environment is protected from external and internal security threats. Because the IT environment is dynamic, vulnerability management is an ongoing process versus a point in time activity.

The responsibility of configuration and patch management falls under several different groups/teams within Equifax: 1) Security, 2) Application Services, 3) Global Corporate Platforms, 4) Risk Programs, and 5) Back office Support (desktop support).

Below is a graph of the current 1000+ Critical/High/Medium Risk Vulnerabilities by age for externally facing systems. These systems are accessible from outside the Equifax network and could be vulnerable to exploitation by hackers.

Page 2

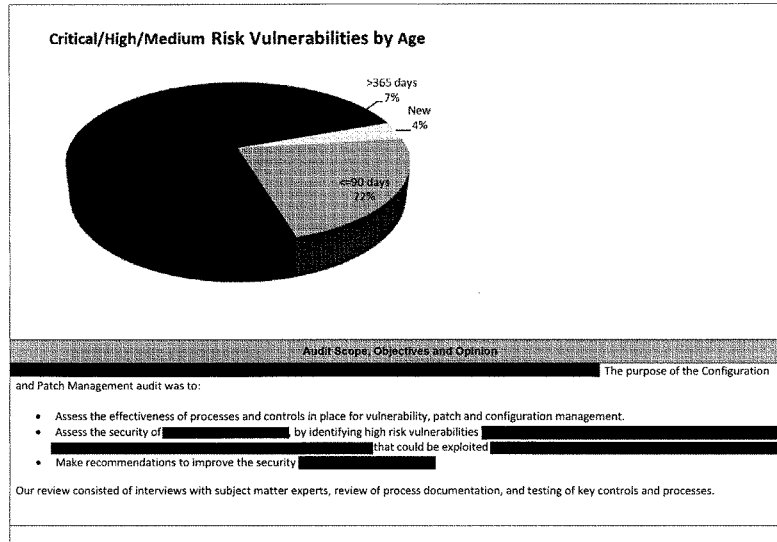
EQUIFAX

Confidential and Proprietary

INFORM » ENRICH » EMPOWER

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
CONTAINS SENSITIVE TECHNICAL AND/OR SECURITY RELATED INFORMATION

EFXCONG-PSI000032257



Page 3

EQUIFAX

Confidential and Proprietary

INFORM › ENRICH › EMPOWER

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
CONTAINS SENSITIVE TECHNICAL AND/OR SECURITY RELATED INFORMATION

EFXCONG-PS/000032258

Detailed Findings and Management Response		
#	Findings	Recommendations
1	<p>Old Vulnerabilities</p> <p>Vulnerabilities are not remediated in a timely manner. There are over 8500 known medium, high or critical vulnerabilities existing with a large percentage of those being over 90 days outstanding. While there are many reasons for the aged vulnerabilities (as detailed in the other findings in this report), one of the factors contributing to the unpatched systems is the large number of [REDACTED]</p> <p>Risk: Lack of timely remediation of vulnerabilities creates a security exposure and could allow Equifax systems and data to be compromised.</p>	<p>Management should implement automated tools to help ensure systems are patched in a timely manner. All existing vulnerabilities should be evaluated to determine what is required to properly remediate the vulnerability. Any systems that can't be remediated should have additional controls implemented to mitigate the security exposure.</p> <p>Management should continue to [REDACTED]</p>
		<p>Management Responses</p> <p><i>Issue Owner:</i> [REDACTED]</p> <p><i>Management Response/Action Plan:</i></p> <ul style="list-style-type: none"> • Leverage/implement automated management products for the [REDACTED] to patch those systems in a consistent manner • [REDACTED] has a mature native patching solution that will continue to be leveraged. • Create a patching cadence that is well understood throughout the COEs and BUs in order to achieve comprehensive patching solution [REDACTED] <p><i>Estimated Remediation Date:</i> 12/31/2016</p>

Detailed Findings and Management Response			
#	Findings	Recommendations	Management Responses
2	<p>Lack of Asset Management/Network Documentation</p> <p>A comprehensive IT asset inventory does not exist nor does accurate network documentation. A global view of the IT infrastructure does not exist across the organization. The lack of an accurate asset inventory makes it difficult to ensure all assets are adequately patched and configured. It also makes it difficult for Information Security to ensure their vulnerability scanning all assets. Without a firm understanding of the status of all IT assets, ensuring the security and stability of Equifax systems is extremely difficult.</p> <p>NOTE: Internal Audit is currently performing an ITAM audit and will issue an audit report in 4Q 2015 that will detail the many aspects that need to be addressed to ensure effective IT asset management procedures are implemented.</p> <p>Risk: Lack of adequate asset management procedures makes it difficult to ensure systems are patched in a timely manner and are being regularly scanned for security vulnerabilities.</p>	<p>Management should improve controls surrounding IT asset management to ensure a current and accurate accounting of all IT assets is available at all times.</p> <p>Accurate network documentation should also be developed and updated on a regular basis.</p>	<p>Issue Owner: [REDACTED]</p> <p>Management Response/Action Plan:</p> <ul style="list-style-type: none"> Form a process improvement initiative [REDACTED] so that it is in the natural flow of our operating models. [REDACTED] [REDACTED] Management responses to the more specific ITAM issues will be included in the ITAM audit report that is to be issued. <p>Estimated Remediation Date: 6/30/2017</p>
3	<p>Reactive Patching Processes</p> <p>Most Equifax systems are not patched in a timely manner. The Security Global Threat and Vulnerability Management (GTVM) team sends out monthly reports notifying IT of necessary security patches and system vulnerabilities. For most of IT, they are using the GTVM information to reactively patch their systems instead of proactively applying patches.</p> <p>[REDACTED]</p>	<p>Management should document and implement a proactive patching process to ensure vendor patches are evaluated, tested, and applied in a timely manner.</p>	<p>Issue Owner: [REDACTED]</p> <p>Management Response/Action Plan:</p> <ul style="list-style-type: none"> Create a patching cadence that is well understood throughout the COEs and BUs in order to achieve comprehensive patching solution. [REDACTED] [REDACTED] [REDACTED] have native products that provide robust capabilities to [REDACTED]

Page 3

EQUIFAX®

Confidential and Proprietary

INFORM » ENRICH » EMPOWER

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
CONTAINS SENSITIVE TECHNICAL AND/OR SECURITY RELATED INFORMATION

EFXCONG-PSI000032260

Detailed Findings and Management Response		
#	Findings	Management Responses
	<p>Risk: By not proactively applying vendor patches, Equifax systems could be vulnerable until GTVM notifies IT of the vulnerability. Additionally, unpatched systems could also impact system performance and availability.</p>	<p>advertise the latest patches and allow for centralized management and enable automation. These will be utilized to help implement a proactive patching process for these environments.</p> <p>• [REDACTED]</p> <p><i>Estimated Remediation Date:</i> 12/31/2016</p>
4	<p>Vulnerability and Exception Tracking</p> <p>Vulnerabilities are not adequately tracked, prioritized and monitored to ensure they are remediated in a timely manner. Monthly meetings are held to notify the IT teams of necessary patches and an honor system is used to ensure the patches are installed. If vulnerability cannot be remediated, the IT owner is responsible for submitting an exception and the Manager of that area is responsible for approving the exception. There are no controls in place to escalate critical vulnerabilities that are not remediated in a timely manner.</p> <p>Risk: Inadequate tracking and escalation of security vulnerabilities could result in Equifax systems being compromised. Additionally, security exceptions should be approved by appropriate levels of Management that are able to properly assess the risk to the business.</p>	<p>Management should implement an exception process to assess, prioritize and monitor all vulnerabilities that do not comply with Equifax policy. The risk and remediation plan for each policy exception should be assessed and approved by the appropriate level of Management and escalated as necessary. When the approved policy exception expires, Security should follow up to ensure the vulnerability was successfully remediated.</p> <p><i>Issue Owner:</i> [REDACTED]</p> <p><i>Management Response/Action Plan:</i> Build and provide a centralized tracking capability. [REDACTED] as an interim solution that might meet our requirements.</p> <p><i>Estimated Remediation Date:</i> Long-term solution is targeted for 2017, unless the interim solution can be fully utilized.</p>
5	[REDACTED]	<p><i>Issue Owner:</i> [REDACTED]</p>

Page 6

Detailed Findings and Management Response			
#	Findings	Recommendations	Management Responses
6	[REDACTED]		
7			

Page 7

EQUIFAX®
Confidential and Proprietary

INFORM › ENRICH › EMPOWER

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
CONTAINS SENSITIVE TECHNICAL AND/OR SECURITY RELATED INFORMATION

EFXCONG-PSI000032262

Detailed Findings and Management Response			
#	Findings	Recommendations	Management Responses
8	<p>Patch Policy</p> <p>The current Patch management policy does not consider the criticality of an IT asset in determining the required time to patch the system. Currently, the policy requires all critical patches be installed in 48 hours, high risk patches within 30 days, medium risk within 90 days, and low risk during the normal patching cycle. Without considering the criticality of the asset containing the vulnerability, the current policy would allow a high risk patch on a critical server 30 days before it is required to be patched.</p> <p>Risk: IT assets classification allows Management to ensure the most critical assets are prioritized from a security and availability perspective. Without appropriate asset classification, critical assets may be vulnerable while less critical assets are being remediated.</p>	<p>The Patch Policy should be enhanced to account for more stringent patching requirements for high risk systems. IT Management should perform a review of all IT assets and classify their risk to the organization.</p>	<p>Issue Owner: [REDACTED]</p> <p>Management Response/Action Plan: We agree that the criticality of the asset is an important factor in determining the priority of patching. Since a new Patching Policy was published by Security in April 2015, we have been working with IT teams globally to implement the Policy. Part of that is to update the Patching Process document. [REDACTED]</p> <p>Estimated Remediation Date: 12/31/2015</p>

Letter From Our President - Updated

January 22, 2016

Dear Starwood Customers:

I am writing to provide you with an update regarding the nature and circumstances of the data security issue we initially announced on November 20, 2015. As indicated in my November 2015 letter, a malware intrusion affected some point of sale systems at a limited number of Starwood hotels in North America. Since that time, we have been working diligently with third-party forensic experts to continue our investigation to help ensure that all impacted hotels have been identified. Based on the continued investigation, we have identified some additional hotels whose point of sale systems were affected by this issue. The updated list of locations and potential dates of exposure for each affected Starwood property is provided [here](#).

As indicated in my prior letter, we discovered that the point of sale systems at certain Starwood hotels were infected with malware, enabling unauthorized parties to access payment card data of some of our customers. We want you to know that the affected hotels have taken steps to secure customer payment card information, and the malware no longer presents a threat to customers using payment cards at our hotels. We also want to assure you that protecting the security of our customers' personal information is a top priority for Starwood.

As indicated in my prior letter, we have determined the following:

- The malware affected certain restaurants, gift shops and other point of sale systems at the relevant Starwood properties. We have no indication that our guest reservation or Starwood Preferred Guest membership systems were impacted.
- The malware was designed to collect certain payment card information, including cardholder name, payment card number, security code and expiration date. There is no evidence that other customer information, such as contact information, Social Security numbers or PINs, were affected by this issue.

We sincerely regret any inconvenience this may cause. We take our obligation to safeguard personal information very seriously and are alerting affected customers about this incident so they can take steps to help protect their information. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe your payment card may have been affected, please contact your bank or card issuer immediately.

In addition, we have arranged with AllClear ID to offer identity protection and credit monitoring services to affected Starwood customers for one year at no cost to them. The [Reference Guide](#) provides information on registration and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

If you have any questions or would like more information, please call 1-855-270-9179 (U.S. and Canada) or 1-512-201-2201 (International), Monday through Saturday, 8:00 am to 8:00 pm CST.

Again, we sincerely apologize for any inconvenience this issue may cause.

Sincerely,

Sergio Rivera
President, The Americas

5/8/2019

Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies - The New York Times

Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies

By Nicole Perlroth

Feb. 18, 2019

SAN FRANCISCO — Businesses and government agencies in the United States have been targeted in aggressive attacks by Iranian and Chinese hackers who security experts believe have been energized by President Trump's withdrawal from the Iran nuclear deal last year and his trade conflicts with China.

Recent Iranian attacks on American banks, businesses and government agencies have been more extensive than previously reported. Dozens of corporations and multiple United States agencies have been hit, according to seven people briefed on the episodes who were not authorized to discuss them publicly.

The attacks, attributed to Iran by analysts at the National Security Agency and the private security firm FireEye, prompted an emergency order by the Department of Homeland Security during the government shutdown last month.

The Iranian attacks coincide with a renewed Chinese offensive geared toward stealing trade and military secrets from American military contractors and technology companies, according to nine intelligence officials, private security researchers and lawyers familiar with the attacks who discussed them on the condition of anonymity because of confidentiality agreements.

A summary of an intelligence briefing read to The New York Times said that Boeing, General Electric Aviation and T-Mobile were among the recent targets of Chinese industrial-espionage efforts. The companies all declined to discuss the threats, and it is not clear if any of the hacks were successful.

Chinese cyberespionage cooled four years ago after President Barack Obama and President Xi Jinping of China reached a landmark deal to stop hacks meant to steal trade secrets.



A 2015 deal between President Barack Obama and President Xi Jinping of China that curtailed hacking intended to steal trade secrets appears to have been unofficially

5/8/2019

Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies - The New York Times

canceled. Doug Mills/The New York Times

But the 2015 agreement appears to have been unofficially canceled amid the continuing trade tension between the United States and China, the intelligence officials and private security researchers said. Chinese hacks have returned to earlier levels, although they are now stealthier and more sophisticated.

"Cyber is one of the ways adversaries can attack us and retaliate in effective and nasty ways that are well below the threshold of an armed attack or laws of war," said Joel Brenner, a former leader of United States counterintelligence under the director of national intelligence.

Federal agencies and private companies are back to where they were five years ago: battling increasingly sophisticated, government-affiliated hackers from China and Iran — in addition to fighting constant efforts out of Russia — who hope to steal trade and military secrets and sow mayhem. And it appears the hackers substantially improved their skills during the lull.

Russia is still considered America's foremost hacking adversary. In addition to meddling widely and spreading disinformation during United States elections, Russian hackers are believed to have launched attacks on nuclear plants, the electrical grid and other targets.

Threats from China and Iran never stopped entirely, but Iranian hackers became much less active after the nuclear deal was signed in 2015. And for about 18 months, intelligence officials concluded, Beijing backed off its 10-year online effort to steal trade secrets.

But Chinese hackers have resumed carrying out commercially motivated attacks, security researchers and data-protection lawyers said. A priority for the hackers, researchers said, is supporting Beijing's five-year economic plan, which is meant to make China a leader in artificial intelligence and other cutting-edge technologies.

"Some of the recent intelligence collection has been for military purposes or preparing for some future cyber conflict, but a lot of the recent theft is driven by the demands of the five-year plan and other technology strategies," said Adam Segal, the director of the cyberspace program at the Council on Foreign Relations. "They always intended on coming back."

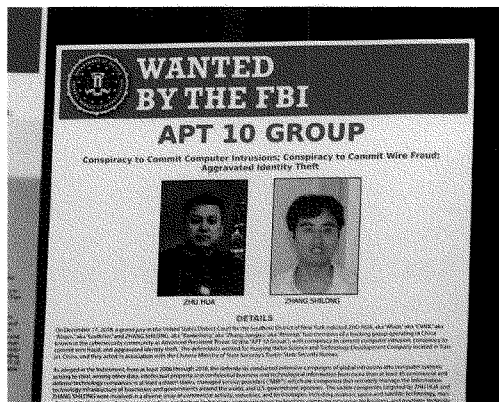
Officials at the Chinese embassy in Washington did not respond to a request for comment.

Mr. Segal and other Chinese security experts said attacks that once would have been conducted by hackers in China's People's Liberation Army are now being run by China's Ministry of State Security.

These hackers are better at covering their tracks. Rather than going at targets directly, they have used a side door of sorts by breaking into the networks of the targets' suppliers. They have also avoided using malware commonly attributed to China, relying instead on encrypting traffic, erasing server logs and other obfuscation tactics.

5/8/2019

Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies - The New York Times



Two Chinese citizens who are suspected of participating in an extensive hacking campaign to steal data from American companies. Manuel Balce Ceneta/Associated Press

"The fingerprint of Chinese operations today is much different," said Priscilla Moriuchi, who once ran the National Security Agency's East Asia and Pacific cyber threats division. Her duties there included determining whether Beijing was abiding by the 2015 agreement's terms. "These groups care about attribution. They don't want to get caught."

It is difficult to quantify the number of industrial-espionage attacks, in part because they have been designed mostly to steal strategic trade secrets, not the kind of personal information about customers and employees that companies must disclose. Only Airbus has acknowledged in recent weeks that Chinese hackers had penetrated its databases.

Many of the attacks by the Chinese Ministry of State Security have been against strategic targets like internet service providers with access to hundreds of thousands, if not millions, of corporate and government networks.

Last week, Ms. Moriuchi, who is now a threat director at the cybersecurity firm Recorded Future, released a report on a yearlong, stealth campaign by the ministry to hack internet service providers in Western Europe and the United States and their customers.

The lone hacking target to publicly confront the ministry was Visma, a Norwegian internet service provider with 850,000 customers. The goal of the attack on Visma was to gain broad access to its customers' intellectual property, strategic plans and emails, including those of an American law firm that handles intellectual property matters for clients in the automotive, biomedical, pharmaceutical and tech sectors, according to Recorded Future.

The Visma attack was harder to trace than earlier incidents, which typically started with so-called spearphishing emails meant to steal personal credentials. This assault began with stolen credentials for a third-party software service, Citrix. And instead of using malware easily traced to China, the attackers used malware available on the so-called Dark Web that could have come from anywhere. They also used the online storage service Dropbox to move stolen emails and files.

Federal agencies are also trying to fend off new Iranian espionage campaigns.

After the Trump administration pulled out of the nuclear deal, Kirstjen Nielsen, the homeland security secretary, testified before Congress that her agency was "anticipating it's a possibility" that Iran would resort to hacking attacks.

5/8/2019

Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies - The New York Times



Stuart Davis, a director at a subsidiary of the security firm FireEye, which has attributed a recent wave of cyberattacks to Iranian hackers. Kanran Jebreili/Associated Press

The Iranian attacks, which hit more than a half-dozen federal agencies last month, still caught the department off guard. Security researchers said the hacks, which exploited underlying weaknesses in the internet's backbone, were continuing and were more damaging and widespread than agency officials had acknowledged.

Iranian hackers began their latest wave of attacks in Persian Gulf states last year. Since then, they have expanded to 80 targets — including internet service providers, telecommunications companies and government agencies — in 12 European countries and the United States, according to researchers at FireEye, which first reported the attacks last month.

The current hacks are harder to catch than previous Iranian attacks. Instead of hitting victims directly, FireEye researchers said, Iranian hackers have been going after the internet's core routing system, intercepting traffic between so-called domain name registrars. Once they intercepted their target's customer web traffic, they used stolen login credentials to gain access to their victims' emails. (Domain name registrars hold the keys to hundreds, perhaps thousands, of companies' websites.)

"They're taking whole mailboxes of data," said Benjamin Read, a senior manager of cyberespionage analysis at FireEye. Mr. Read said Iranian hackers had targeted police forces, intelligence agencies and foreign ministries, indicating a classic, state-backed espionage campaign rather than a criminal, profit-seeking motive.

There is a long history of Iranian attacks against the United States, and episodes from five years back or longer are just now being made public.

On Wednesday, the Justice Department announced an indictment against a former Air Force intelligence specialist, [Monica Witt](#), on charges of helping Iran with an online espionage campaign. Four members of Iran's Islamic Revolutionary Guard Corps were also charged with "computer intrusions and aggravated identity theft" directed at members of the United States intelligence community.

Also last week, the Treasury said it was putting sanctions on two Iranian companies, New Horizon Organization and Net Peygard Samavat Company, and several people linked to them. Treasury officials said New Horizon set up annual conferences where Iran could recruit and collect intelligence from foreign attendees.

5/8/2019

Iranian Hackers Have Hit Hundreds of Companies in Past Two Years - WSJ

BUSINESS

Iranian Hackers Have Hit Hundreds of Companies in Past Two Years

Cyberattack campaign has caused damages estimated at hundreds of millions of dollars, focusing on Middle East but also affecting U.S.



Italian oil company Saipem was hit by the hackers. PHOTO: IGOR GOLOVNIOV/SOPA IMAGES/ZUMA PRESS

By Robert McMillan

Updated March 6, 2019 7:28 p.m. ET

Cyberattacks linked to Iranian hackers have targeted thousands of people at more than 200 companies over the past two years, Microsoft Corp. MSFT +0.02% said, part of a wave of computer intrusions from the country that researchers say has hit businesses and government entities around the globe.

The campaign, the scope of which hadn't previously been reported, stole corporate secrets and wiped data from computers. It caused damages estimated at hundreds of millions of dollars in lost productivity and affected oil-and-gas companies, heavy-machinery manufacturers and international conglomerates in more than a half-dozen countries including Saudi Arabia, Germany, the U.K., India and the U.S., according to researchers at Microsoft, which deployed incident-response teams to some of the affected companies.

"These destructive attacks...are massively destabilizing events," said John Lambert, the head of Microsoft's Threat Intelligence Center.

Microsoft traced the attacks to a group it calls Holmium. It is one of several linked by other researchers over the past year to hackers in Iran, a country that many security researchers say aspires to join Russia and China as one of the world's premier cyber powers. Some of Holmium's hacking was done by a group that other security companies call APT33, Microsoft said.

Iran "denies any involvement in cyber crimes against any nation," said a spokesman for Iran's mission to the United Nations in an email. He called the cybersecurity research by Microsoft and other companies "essentially ads, not independent or academic studies," that should not be taken at face value.

While American and European companies have been hit, security researchers say the attacks from Iran have focused heavily on the Middle East.

But they say Iran's growing cyber strength poses a potential threat to the U.S. at a time of intensified tension between the two countries.

"They're definitely sharpening their skills and moving up their capabilities," said John Hultquist, director of intelligence analysis at the cybersecurity firm FireEye Inc. "When they turn their attention back to the United States, we may be surprised by how much more advanced they are."

One target hit by APT33 is Italian oil company Saipem SPM 1.35% SpA. A December attack wiped data and affected computer infrastructure at company facilities in the Middle East, India, Scotland and Italy, according to Saipem.

Microsoft has been tracking Holmium for nearly four years. Activity surged in late 2018, according to Microsoft and other companies following the group.

To date, Mr. Lambert and his researchers have seen Holmium target more than 2,200 people across about 200 organizations with phishing emails that, if clicked, can install code that steals information or wipes data from computers on the victim's network.

In a phishing email sent to a victim and viewed by The Wall Street Journal, Holmium attackers copied a legitimate job advertisement from a Saudi Arabian oil-and-gas company and sent it to a worker with oil-industry expertise. When clicked on, the email led to a website that then attempted to download malicious software onto the victim's computer.

In January, FireEye warned that Iran-linked hackers were using another technique to break into corporate networks, hitting an "almost unprecedented" number of victims world-wide with a high

degree of success.

FireEye said in a blog post that the hackers had been manipulating the critical DNS, or domain name service, records of companies—often telecommunications and internet service providers based in the Middle East—monitoring targets’ internet traffic to read email messages and steal usernames and passwords.

FireEye observed at least 50 entities—including corporations, universities and government agencies—hit by this attack, but said it suspected many more victims.

Two weeks after FireEye’s warning, the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency issued a warning about this type of attack, saying the technique, called DNS hijacking, was also being used against the U.S. government.

However, security researchers, including FireEye, say there isn’t enough evidence to know whether Iran was involved in the U.S.-focused attacks or hackers from a different country launched them using the same techniques.

Researchers agree that the Iran-linked attacks don’t rely on “zero day” exploits, or those leveraging previously undisclosed flaws in computer products. Zero-day attacks are the hallmark of elite hacking groups.

While the attacks tied to Iran use less sophisticated tactics, they often cast a wide net.

Last year, Facebook Inc. removed dozens of pages that it had tied to an Iranian influence operation. Months before that, federal authorities charged nine Iranians with launching cyberattacks that hit 144 American universities, 36 U.S. companies and five American government agencies between 2013 and 2017.

Symantec Corp. tracked another campaign it linked to Iran in which hackers went after 800 organizations over the course of the past two years. The unusually large target list shows that the hackers aren’t using the kind of precise targeting typically associated with a nation-state attacker, said Vikram Thakur, a researcher with Symantec. Typical nation-state campaigns would focus on fewer than 100 entities, he said.

“No one attacks 800 organizations on purpose,” he said. “It just shows that these people were being very opportunistic.”

5/8/2019

Iranian Hackers Have Hit Hundreds of Companies in Past Two Years - WSJ

Another Iranian-linked group also has hit more than 200 government agencies, oil-and-gas companies and technology companies including Citrix Systems Inc., according to the security firm Resecurity International Inc. Using a technique described in an alert issued by the Department of Homeland Security last year, the hackers guess the passwords for corporate email accounts, then steal data that they use to burrow further into corporate networks.

A Citrix spokesman confirmed that a single employee account was compromised in 2018 due to a weak password and that the hacker then used that access to obtain “an old version of a list containing Citrix employee work contact information.”

The Citrix attack is worrying because the software maker builds widely used remote-access products that could be misused by hackers to gain unauthorized access to other corporate networks. Citrix says it has seen no evidence of any compromise beyond that single account. The company has also “not found any evidence of state-sponsored activity,” the spokesman said in an email.

Write to Robert McMillan at Robert.Mcmillan@wsj.com

Appeared in the March 7, 2019, print edition as 'Iranian Hackers Hit Companies.'

Appendix A**CLARIFICATIONS AND PROPOSED EDITS TO THE TESTIMONY OF MARK
BEGOR AND JAMIL FARSHCHI AT THE MARCH 7, 2019 HEARING OF THE
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS**

During the hearing, Senator Harris asked Mr. Begor a question premised on the possibility that a foreign nation state was responsible for the cybersecurity incident. In response, Mr. Begor testified that “we don’t know who took the data” To clarify, Equifax is not able to identify the attackers responsible for the cybersecurity incident. Federal law enforcement has been investigating the attack, and Equifax hopes that they will have sufficient evidence to identify and prosecute the attackers. Equifax continues to cooperate with law enforcement as necessary to assist that effort.

During the hearing, Senator Peters asked Mr. Begor whether Equifax had any policies regarding the collection of information on minors. In response, Mr. Begor testified that Equifax’s policy is to not collect information on minors, and that Senate Bill 2155 allows parents to place “a freeze on their children’s credit file, if in fact, they have one.” To clarify, Equifax’s policy is not to collect data on minors. However, under Senate Bill 2155 and Equifax’s Family Plan, parents may elect to share minor information with Equifax for the purpose of freezing or locking their minor child’s credit file, regardless of whether a credit file exists. If a file does not already exist, Equifax will create a file to freeze or lock it.

Equifax has also submitted an edited copy of the transcript directly to the Subcommittee Clerk, as requested in her March 22, 2019 cover letter conveying the official transcript to Equifax.

Appendix B

**SUBMISSION IN RESPONSE TO SUBCOMMITTEE QUESTIONS
FOR THE RECORD DATED MARCH 22, 2019**

Written Questions for the Record from Senator Kamala D. Harris

- Question 1:** If a hostile foreign power is using the data it stole from Equifax to target U.S. officials or American operatives, does it remain Equifax's position that there has been no injury or harm caused by the breach?
- Question 2:** It remains a concern that foreign actors target private sector entities, like Equifax, to obtain sensitive information for the purposes of compromising American military and intelligence personnel. What steps is Equifax taking to mitigate the risk to U.S. national security professionals posed by the 2017 data breach?
- Question 3:** How has Equifax made understanding the harm that has resulted from its previous data breaches a priority among its security efforts in the wake of its 2017 data breach?

Response: Equifax is unable to opine whether the 2017 cybersecurity incident resulted in heightened risk or actual harm or injury for U.S. officials, operatives, and national security professionals. However, Equifax has cooperated fully with law enforcement in its investigation of the incident and remains fully committed to doing so going forward. Equifax welcomes the opportunity to engage with this Subcommittee, federal law enforcement, and other government entities regarding potential additional measures to mitigate any risk to U.S. officials, operatives, and national security professionals that may arise from cybersecurity attacks.

Written Questions for the Record from Senator Kyrsten Sinema

- Question 1:** In your testimony, you state that Equifax has not identified any evidence indicating the sale of any stolen information from the 2017 breach. You also note that cybercrime is increasingly sophisticated and performed by well-funded nation state actors. Given that the data of 145 million Americans has effectively disappeared, is it more likely that the breach was conducted by independent criminals or a nation state?

Response: Equifax is not able to identify the attackers responsible for the cybersecurity incident. Federal law enforcement has been investigating the attack, and Equifax hopes that they will have sufficient evidence to identify and prosecute the attackers. Equifax continues to cooperate with law enforcement as necessary to assist that effort.

Question 2: In your testimony, you state that Equifax did not fail to take cybersecurity seriously prior to the 2017 breach. However, Equifax took two months to address web-application vulnerabilities and six weeks to notify the public of the breach. The Subcommittee's report also demonstrates a general neglect of cybersecurity protocol starting in 2015. With these facts in mind, how are you able to confidently defend Equifax's 2017 commitment to cybersecurity?

Response: Prior to the breach, Equifax expended significant resources and effort in maintaining a reasonable security program prior to the cybersecurity incident. Among other things, the program was appropriately resourced, staffed, and structured; it had a comprehensive set of policies, standards, and procedures; it featured robust training and periodic security exercises; it was comprised of appropriate technical security controls, including with respect to vulnerability and threat management; and it was subject to regular evaluation and improvement through external and internal assessments. The fact that the Company suffered a breach does not mean that the Company did not take cybersecurity seriously.

Question 3: In your testimony, you discuss Equifax's efforts to provide consumers greater control over their personal data. Equifax's Lock & Alert™ service allows consumers to lock and unlock their Equifax credit reports on a mobile application. However, freezing one's data does not necessarily equate to controlling how that data is collected and disseminated. Privacy experts have noted that locking your report still allows the credit bureau to access your data and distribute it for marketing purposes. Additionally, applying for credit requires your account remain unlocked for potential lenders. Can you explain how Lock & Alert™ allows consumers to control their data in a meaningful way?

Response: Equifax's Lock & Alert service gives consumers the ability to unlock and lock their Equifax credit reports for free, for life. At its most basic level, a credit lock like Lock & Alert does the same thing as a credit freeze; it prevents certain access to a consumer's Equifax credit report by creditors and lenders, and helps prevent the opening of unauthorized new accounts. Unless a consumer gives permission or takes action by unlocking the account, a lender or other creditor cannot access the consumer's Equifax credit report for the purposes of opening new credit accounts.

Question 4: How should private entities that suffer a data breach notify affected consumers, law enforcement, and the appropriate federal agencies in a timely fashion?

- a. Would you support federal legislation which accomplished those goals?
- b. What key factors should Congress consider when crafting this legislation?

Response: Yes. A single federal breach notification standard would help ensure that all impacted consumers and regulators receive the same information regarding a breach incident in an efficient and expedient manner. Lawmakers may want to consider key elements in developing a federal standard including:

- **Regulator Notices & Enforcement:** Some states require notice be provided to the state's Attorney General or other state agencies. A federal breach law may want to consider consolidating regulator notices to a single federal authority to streamline the initial notification, centralize follow up requests and information regarding the incident, coordinate communication among various stakeholders, and ultimately, enforce a federal breach notification standard.
- **Direct and Substitute Notices:** All state statutes provide for a substitute or alternate notice versus a direct notice to consumers depending on the cost of a direct notice, the universe of affected consumers residing in the state, or the lack of sufficient contact information for the consumers. States agree that flexibility is important when considering notification, and that all breach incidents should not necessarily require a direct notification to all impacted consumers.
- **Timing:** Many states require notification "in the most expedient time and manner possible and without unreasonable delay" following the discovery of a breach (for example, New York and California data breach statutes). This guidance allows the breached entity time to determine the scope of the incident and the number of consumers impacted, and to restore the integrity of systems before moving forward with public notification. While a minority of states require notice within a specific time frame, generally between 30 to 45 days, most states recognize that it is important for a breached entity to conduct an investigation and to complete corrective actions before providing notification. This will help ensure that the security or technological vulnerability has been addressed and the breach notification is provided to the correct consumers and includes the most accurate information regarding the incident.
- **Content Notification:** Most states requires the same general content requirements, and allow for a breached entity to provide a "standard" letter to a majority of impacted consumers that meets the requirements including the date of the breach; general description of the incident; type of PII impacted, contact information for the entity; contact information for the consumer reporting agencies: the FTC and Attorneys General; steps taken to prevent a further breach; and advice to consumers to remain vigilant including reviewing account statements, reporting unauthorized activity to law enforcement and information regarding fraud alerts and security freezes. Some states, however, have state-specific requirements that typically require separate form notification letters, as noted in the response above. Consistent content notification requirements across all states

would ensure that consumers receive the same information regarding a breach incident regardless of where they reside. Further, the breached entity would likely be able to make the disclosure more quickly and efficiently, to the benefit of consumers.

Other provisions to consider when evaluating a federal breach notification standard should include whether PII is “acquired” versus “accessed,” the breached entity is a “data owner” versus a “maintainer,” the definition of PII, a risk of harm analysis, data encryption, and “electronic” versus “paper records.”

* * *

**Post Hearing Questions for the Record
Submitted to Arne M. Sorenson
President and Chief Executive Officer
Marriott International, Inc.
From Senator Jacky Rosen**

**“Examining Private Sector Data Breaches”
Senate Committee on Homeland Security and Governmental Affairs
Permanent Subcommittee on Investigations
March 7, 2019**

In August 2017, Marriott International, Inc. announced a joint venture with Chinese tech giant Alibaba to leverage Marriott International’s global portfolio of brands and unparalleled hospitality expertise to revolutionize the travel experience as well as Alibaba’s digital retail leadership and its role as a gateway for international brands to reach over 500 million mobile monthly active users across its platform.

- **Please provide more detail on how the joint venture will “manage Marriott’s storefront, on Fliggy, Alibaba’s travel service platform.”**

RESPONSE: Marriott and a subsidiary of Alibaba established a joint venture effective August 1, 2017 to manage Marriott’s storefront on Fliggy, Alibaba’s travel service platform, in an effort to reach consumers in China. The joint venture entity, Travel Ease, conducts business in China under the trade name Wei-yo. Marriott has a 49% stake in the joint venture entity with two representatives on the Board, while Alibaba has a 51% stake with three Board representatives. Wei-yo was established for the development and management of a dedicated on-line storefront within Fliggy’s platform (the “Storefront”), a Marriott Chinese website, and a Chinese mobile app, as well as creation of marketing content, packages and vouchers. At present, the Storefront is the only active channel managed by Wei-yo. Wei-yo is also focusing on content, packages and vouchers developed for the Storefront, and targeting customers in China. The website and mobile app that were initially contemplated for management by Wei-yo have not been established.

- **Please describe in more detail the “link between Marriott’s loyalty programs and Alibaba’s loyalty programs.”**

RESPONSE: Both Marriott’s and Alibaba’s loyalty programs are activated when a guest makes a reservation for a hotel or package developed by Wei-yo and offered on the Storefront. Customers can enroll in Marriott Bonvoy through the membership page on the Storefront. To facilitate the enrollment process, Alibaba sends relevant enrollment information in its possession (including name and cellphone number) to Wei-yo, which then obtains the associated Marriott Bonvoy loyalty program number for the customer. The new member is then asked to provide additional information as necessary to complete enrollment (e.g. e-mail address) and set up a password. Upon enrollment, the customer is assigned a Marriott Bonvoy membership level that is commensurate with the

customer's Fliggy membership status. Marriott Bonvoy members can then earn Marriott Bonvoy points for rooms booked at member rates on the Storefront.

- **Will U.S. travelers in China use the same features that the joint venture plans to aim at Chinese travelers, i.e., frictionless planning, booking, paying, and managing a trip; personalized and VIP experiences; wallet-free travel; and use of Marriott's loyalty platform in hotels located in China?**

RESPONSE: While U.S. travelers visiting China may book travel through Fliggy's Storefront, they are unlikely to do so because the platform is in Simplified Chinese and, in order to make the booking, the customer must have an Alibaba Alipay mobile payment account. The primary goal of using the Storefront is to reach Chinese-speaking customers in China and provide products based on Chinese consumer demands that may not be the same for U.S. travelers. Accordingly, U.S. travelers booking through other websites may not have access to the same offerings.

- **Will the joint venture manage the reservations of U.S. travelers in China who stay at Marriott hotels or their affiliates? If so, will Alibaba have access to personal identifiable information (PII) of those U.S. travelers?**

RESPONSE: The joint venture does not manage reservations made by U.S. travelers in China through channels outside of the Fliggy platform. To use the Fliggy platform, a customer must be a registered user with Alibaba and a new customer must register to become one. If a U.S. customer chooses to make a reservation through the Fliggy platform, the customer will be using or creating an Alibaba account, providing his or her information to Alibaba, and will then be subject to Alibaba's privacy policies.

- **Will Alibaba have access to personal identifiable information (PII) of U.S. customers, whether or not they travel to China, through the "link" between Alibaba's and Marriott's loyalty programs?**

RESPONSE: An Application Program Interface connects Alibaba's Fliggy platform to Netlink, which feeds information to the Marriott customer database. The connection as currently set up does not give Alibaba access to information in Marriott's customer database.

Does Marriott use facial recognition for hotel check-in at China hotels? If so, please describe Marriott's policies for storing data obtained using facial recognition technology.

RESPONSE: Marriott hotels in China comply with local law requirements. In certain provinces in China, the Chinese government has requirements on collection of guest biometric data. For example, in Shanghai, Guangdong, Zhejiang, and Sanya, upon check-in, guests are scanned by a facial recognition scanner connected to the government's database. Biometric data is sent directly to the Police Bureau as required by the Chinese authorities. Marriott does not store this data.

Additionally, at two Marriott properties in Sanya and Hangzhou, facial recognition machines provided by Fliggy are available for the convenience of guests to expedite the check-in process. Marriott does not store guests' facial recognition data, which is sent directly to the Police Bureau. Guests opting to use this technology must sign the terms of service and scan their Chinese government-issued identification to verify their identity. All other guests complete registration through the regular check-in process.