S. HRG. 115–401

PROTECTING CONSUMERS IN THE ERA OF MAJOR DATA BREACHES

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

NOVEMBER 8, 2017

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
33–395 PDF WASHINGTON : 2018

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi	BILL NELSON, Florida, *Ranking*
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	RICHARD BLUMENTHAL, Connecticut
JERRY MORAN, Kansas	BRIAN SCHATZ, Hawaii
DAN SULLIVAN, Alaska	EDWARD MARKEY, Massachusetts
DEAN HELLER, Nevada	CORY BOOKER, New Jersey
JAMES INHOFE, Oklahoma	TOM UDALL, New Mexico
MIKE LEE, Utah	GARY PETERS, Michigan
RON JOHNSON, Wisconsin	TAMMY BALDWIN, Wisconsin
SHELLEY MOORE CAPITO, West Virginia	TAMMY DUCKWORTH, Illinois
CORY GARDNER, Colorado	MAGGIE HASSAN, New Hampshire
TODD YOUNG, Indiana	CATHERINE CORTEZ MASTO, Nevada

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

CONTENTS

PROTECTING CONSUMERS IN THE ERA OF MAJOR DATA BREACHES

WEDNESDAY, NOVEMBER 8, 2017

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:04 a.m. in room SD–106, Dirksen Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Wicker, Blunt, Moran, Sullivan, Heller, Capito, Gardner, Young, Nelson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Udall, Peters, Baldwin, Duckworth, Hassan, and Cortez Masto.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning. Now that our executive session is complete, we turn to the issue of data breaches.

Data breach is not a new issue for the Committee to explore. In fact, the Committee has been focused on the consumer impact of data breaches since before I was elected to the U.S. Senate.

The September 2004 ChoicePoint breach, what many consider to be the first high-profile data breach of the modern era, prompted a number of investigations from this Committee, from the FTC, and from Federal and state authorities.

For those that don't remember, ChoicePoint was a data aggregation company originally created by Equifax, who, as fate would have it, is represented here today. In terms of the trajectory of congressional inquiry into major data breaches, you might say we've come full circle.

In the intervening years, Congress, and this Committee in particular, have paid close attention to data breaches big and small. In addition, the Committee has entertained a variety of proposals to strengthen data security requirements for companies across the board, as well as to impose Federal requirements for affected companies to notify their consumers following the discovery of a breach.

Sadly, we are truly in the era of major data breaches. These include the large-scale breaches at Equifax and Yahoo! that we are examining today.

While the Yahoo! breaches are larger in terms of affected consumers, the Equifax breach is potentially much more severe given the sensitive nature of the consumer information compromised. In fact, I've heard from many constituents in South Dakota who are

concerned about the lasting effects of the Equifax breach. I have also heard complaints that it is difficult to set up a credit freeze, and questions about whether credit monitoring is an effective tool to prevent identity theft.

The Equifax breach reportedly exposed the sensitive personal data of about 145.5 million U.S. consumers, including their names, Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers.

Also exposed were the credit card numbers for more than 200,000 U.S. consumers and dispute documents containing personal identifying information for more than 180,000 U.S. consumers.

Today, Equifax will have an opportunity to provide an update regarding the breach, as well as its much-criticized efforts to mitigate the harm and prevent anything like this from happening again.

The Yahoo! breach we will discuss today compromised over 3 billion user accounts and followed a prior breach in which hackers stole similar types of information from at least 500 million users. The compromised data included names, telephone numbers, dates of birth, partial passwords, unencrypted security questions and answers, backup e-mail addresses, and employment information. The 3 billion figure constitutes the entirety of the Yahoo! Mail and other Yahoo!-owned accounts at the time of the breach.

Today, Yahoo! representatives will have an opportunity to provide an update regarding these breaches as well as efforts to mitigate the harm and ensure the security of consumer data going forward.

The massive data breaches at Equifax and Yahoo! illustrate quite dramatically that our Nation continues to face constantly evolving cyber threats to our personal data. Companies that collect and store personal data on American citizens must step up to provide adequate cybersecurity, and there should be consequences if they fail to do so.

The Committee has made cybersecurity a priority, and I am hopeful that today's hearing will help the Committee to better understand these challenges as it considers legislation to address data breach notification and data security issues.

When there is a risk of real harm stemming from a breach, we must make sure that consumers have the information that they need to protect themselves. That's why I support a uniform Federal breach notification standard to replace the patchwork of laws in 48 states in addition to the District of Columbia and three other territories.

A single Federal standard would ensure all consumers are treated the same with regard to notification of data breaches that might cause them harm. Such a standard would also provide consistency and certainty regarding timely notification practices benefiting both consumers and businesses.

In order to ensure that businesses secure information appropriately, I have also advocated for uniform reasonable security requirements to protect consumer data, based on the size and scope of the company and the sensitivity of the information. However, in this regard, the facts of the Equifax breach are particularly troubling.

As a credit bureau, Equifax was already subject to the Safeguards Rule under the Gramm-Leach-Bliley Act, which is considered to be a stringent regulation. Nevertheless, the Equifax breach occurred, and its implications on American consumers appear dire.

Enhancing security and protecting the personal data of American consumers will continue to be a priority for this Committee. So I want to thank all of our witnesses for appearing here today. And I look forward to hearing your testimony.

I will now turn to Senator Nelson for his opening remarks.

[The prepared statement of Senator Thune follows:]

PREPARED STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Good morning. Now that our executive session is complete, we turn to the issue of data breaches.

Data breach is not a new issue for the Committee to explore. In fact, the Committee has been focused on the consumer impact of data breaches since before I was elected to the U.S. Senate.

The September 2004 ChoicePoint breach, what many consider to be the first high-profile data breach of the modern era, prompted a number of investigations from this Committee, the FTC, and Federal and state authorities.

For those that don't remember, ChoicePoint was a data aggregation company originally created by Equifax, who as fate would have it, is represented here today. In terms of the trajectory of congressional inquiry into major data breaches, you might say we have come full circle.

In the intervening years, Congress, and this Committee in particular, have paid close attention to data breaches big and small. In addition, the Committee has entertained a variety of proposals to strengthen data security requirements for companies across the board, as well as to impose Federal requirements for affected companies to notify their consumers following the discovery of a breach.

Sadly, we are truly in the era of major data breaches. These include the large-scale breaches at Equifax and Yahoo! that we are examining today.

While the Yahoo! breaches are larger in terms of affected consumers, the Equifax breach is potentially much more severe given the sensitive nature of the consumer information compromised. In fact, I have heard from many constituents in South Dakota who are concerned about the lasting effects of the Equifax breach. I have also heard complaints that it is difficult to set up a credit freeze, and questions about whether credit monitoring is an effective tool to prevent identity theft.

The Equifax breach reportedly exposed the sensitive personal data of about *145.5 million U.S. consumers,* including their names, social security numbers, birth dates, addresses, and in some cases, driver's license numbers.

Also exposed were the credit card numbers for more than 200,000 U.S. consumers and dispute documents containing personal identifying information for more than 180,000 U.S. consumers.

Today, Equifax will have an opportunity to provide an update regarding the breach, as well as its much-criticized efforts to mitigate the harm and prevent anything like this from happening again.

The Yahoo! breach we will discuss today compromised over *3 billion user accounts* and followed a prior breach in which hackers stole similar types of information from at least *500 million users.*

The compromised data included names, telephone numbers, dates of birth, partial passwords, unencrypted security questions and answers, backup e-mail addresses, and employment information.

The *3 billion* figure constitutes the entirety of the Yahoo! Mail and other Yahoo!-owned accounts at the time of the breach.

Today Yahoo! representatives will have an opportunity to provide an update regarding these breaches as well as efforts to mitigate the harm and ensure the security of consumer data going forward.

The massive data breaches at Equifax and Yahoo! illustrate quite dramatically that our Nation continues to face constantly evolving cyber threats to our personal data.

Companies that collect and store personal data on American citizens must step up to provide adequate cybersecurity. And there should be consequences if they fail to do so.

The Committee has made cybersecurity a priority, and I am hopeful that today's hearing will help the Committee to better understand these challenges as it considers legislation to address data breach notification and data security issues. When there is risk of real harm stemming from a breach, we must make sure that consumers have the information they need to protect themselves.

That is why I support a uniform Federal breach notification standard to replace the patchwork of laws in 48 states, in addition to the District of Columbia and three other territories.

A single Federal standard would ensure all consumers are treated the same with regard to notification of data breaches that might cause them harm. Such a standard would also provide consistency and certainty regarding timely notification practices, benefiting both consumers and businesses.

In order to ensure that businesses secure information appropriately, I have also advocated for uniform, reasonable security requirements to protect consumer data, based on the size and scope of the company and the sensitivity of the information.

However, in this regard, the facts of the Equifax breach are particularly troubling. As a credit bureau, Equifax was already subject to the Safeguards Rule under the Gramm-Leach-Bliley Act, which is considered to be a stringent regulation.

Nevertheless, the Equifax breach occurred and its implications on American consumers appear dire.

Enhancing security and protecting the personal data of American consumers will continue to be a priority for this Committee. I want to thank all of the witnesses for appearing here today. I look forward to hearing your testimony.

I will now turn to Senator Nelson for his opening remarks.

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman. This, as you stated, is the latest edition in the long history of hearings that we've held on this Committee to discuss data security and breaches.

I want to thank several Senators on this Committee who have asked for this hearing, including Senator Baldwin in particular, and Senator Cortez Masto. Thank you for all the more bringing this to the forefront.

If you start with the massive breach of the ChoicePoint breach in 2005, continuing with Target, Neiman Marcus, Snapchat, Sony, Citigroup, CVS, South Shore Hospital, Heartland Payment Systems, and many, many others, the parade of high-profile data breaches seems to have no end. Billions of consumers have had their sensitive personal, personally identifiable information compromised, including Social Security numbers, driver's licenses, addresses, dates of birth.

For years going forward, criminals can use this data to steal the identity of innocent consumers and create fake accounts in their names and commit other types of fraud. I might point out that right now we estimate $5 billion a year is being stolen from the U.S. Treasury just on fake Federal income tax returns of which they get a refund.

On top of that, we also recently found out the 2013 Yahoo! breach compromised the personal data, it's hard to believe, of 3 billion users. That's the biggest data breach in history. And yet today, here we are once again dealing with the aftermath of the recent Equifax breach involving the personal identification information of nearly 145 million Americans.

Now, this most recent breach raises an even more troubling question because if credit reporting agencies that offer identity theft protection and credit monitoring services can't even safeguard their own data from hackers, then how can consumers trust any

company to protect their information? Let me say also when you get up against the sophistication of state actors such as Russia and China, it's going to be hard to protect against them.

Sadly, the question that millions of Americans are now asking is, as they struggle to figure out how to protect themselves in the wake of these massive breaches, "What in the world do we do?"

So this Committee, Mr. Chairman, is going to again consider what it would do to make sure that consumers are protected. But if we're going to do anything meaningful, we must have the political will to hold these companies accountable.

Over the years, the Federal Trade Commission has brought numerous enforcement actions against companies for lax data security practices, but industry has recently challenged the FTC's well-established legal authority to bring such actions.

Furthermore, this piecemeal, after-the-fact approach would be better served if the FTC were able to prescribe rules that require companies to adopt reasonable security practices in the first place. The FTC has already put forward rules that apply to financial institutions like Equifax. The agency should have a similar authority for the rest of the commercial sector.

Mr. Chairman, I think at the end of the day, only stiffer enforcement and stringent penalties are going to be able to help incentivize companies to properly safeguard their consumer information and to notify their consumers when they've been compromised. I strongly believe that without rigorous data security rules in place, it is not a question of if that we will have another breach, but when.

We can either take action with commonsense rules, or we can start planning for our next hearing on this issue.

Thank you, Mr. Chairman.

[The prepared statement of Senator Nelson follows:]

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Thank you, Mr. Chairman, and thank you for holding this important hearing.

Mr. Chairman, this is the latest edition in a long history of hearings we've held in this Committee to discuss data security and breaches. Starting with the massive ChoicePoint breach in 2005, and continuing with Target, Neiman Marcus, Shapchat, Sony, Citigroup, CVS, South Shore Hospital, Heartland Payment Systems, and many, many others, the parade of high-profile data breaches seems to have no end.

And here we are once again, today, dealing with the aftermath of what is by most accounts the most serious data breach to date. Over 145 million consumers have had their sensitive personal data compromised, including Social Security numbers, drivers' license numbers, addresses, dates of birth. For years going forward, criminals can use this data to steal the identity of innocent consumers and create fake accounts in their names and commit other types of fraud.

On top of that, we also recently found out that the 2013 Yahoo breach compromised the personal data of 3 billion users, making it the biggest data breach in history.

The repercussions of these massive breaches will probably not be fully understood for many years. As consumers struggle to figure out how to protect themselves in the wake of these massive breaches, this committee will, no doubt, once again, consider what it can do to make sure consumers are protected from these breaches. But if we are going to do anything meaningful, Congress must have the political will to hold these corporations accountable.

Over the years, the Federal Trade Commission has brought numerous enforcement actions against companies for lax data security practices. But industry has recently challenged the FTC's well-established legal authority to bring such enforcement actions. Furthermore, this piecemeal, after-the-fact approach would be better served if the FTC were able to prescribe rules that require companies to adopt rea-

sonable security practices in the first place. The FTC has already promulgated such rules under the Gramm Leach Bliley Act that apply to financial institutions like Equifax. The agency should have similar authority for the rest of the commercial sector.

That is why I intend to re-introduce the Data Security and Breach Notification Act, which Senator Blumenthal and I introduced in the last Congress. Only stiffer enforcement and stringent penalties will help incentivize companies to properly safeguard consumer information and promptly notify them when their data has been compromised.

Mr. Chairman, I strongly believe that without such rigorous data security rules in place, the next massive data breach is right around the corner. So we can either take action to enact these common-sense rules or we can start planning for our next hearing on this issue, because it's not going away on its own.

The CHAIRMAN. Thank you, Senator Nelson. And I, too, hope that the hearing today can inform our future actions. It's an issue that I think needs to be addressed, and Congress needs to be heard from.

So I'm glad to have our panel with us this morning. On my left, and your right, is Mr. Paulino do Barros, Jr., who is the Interim Chief Executive Officer at Equifax. Next to him is Mr. Richard Smith, who is the former CEO at Equifax; Ms. Marissa Mayer, who is the former CEO at Yahoo!, Incorporated; Ms. Karen Zacharia, who is the Deputy General Counsel and Chief Privacy Officer for Verizon Communications Incorporated, the parent company of Yahoo! since 2017; and Mr. Todd Wilkinson, who is President and Chief Executive Officer of Entrust Datacard Corporation.

So we'll ask you to proceed with your comments. I'll start on my left with you, Mr. Barros, and ask, if you can, to confine your oral remarks as close to 5 minutes as possible, but anything that you want to add will be included in the written record of the hearing. So thank you for being here.

Mr. Barros.

STATEMENT OF PAULINO DO REGO BARROS, JR., INTERIM CHIEF EXECUTIVE OFFICER, EQUIFAX, INC.

Mr. BARROS. Good morning. Chairman Thune, Ranking Member Nelson, members of the Committee, thank you for the opportunity to be here today. My name is Paulino do Rego Barros, Jr. Six weeks ago, I was named interim Chief Executive Officer of Equifax. I never expected to become CEO in these circumstances, but I am honored to be in this position. Speaking for everyone at Equifax, I'm determined to address all the issues from the data breach, so that we can regain the confidence of the American people.

Although Equifax is based in Atlanta, I think you can tell from my accent that I did not grow up in Georgia. I'm a native of Brazil. I have had the privilege of working most of my adult life in the U.S. My children were born here. I'm an engineer by training, and I have spent a lifetime confronting and fixing complex business problems. This is the mindset I bring to my new position.

My first act as CEO was to immediately address our consumer response in the call centers and our website. Our engagement with consumers was not acceptable, and we are working hard to fix the problems.

I also apologized to the American people, and I do so again here today. What I promise each of you and the American people is that Equifax will be focused every day on strengthening security and

providing better support for consumers. We will be an industry leader in giving consumers more control over personal credit data.

In advance of your questions, I would like to review briefly some of the actions we have taken in the past 6 weeks.

First, my highest priority has been to improve service for consumers. To this end, I have visited call centers, spoken with call center representatives, personally taken calls from consumers, and helped resolve their issues. Through social media, we have expanded communications with consumers. Most significantly, we have improved the website, added staff to call centers, and made the overall experience more consumer-friendly. The result is a substantial reduction in delays and backlogs.

Second, we have revised our corporate structure. The Chief Security Officer now reports directly to me. I have also appointed a Chief Transformation Officer to oversee the company's response to the cybersecurity incident.

Third, we are rapidly improving our security infrastructure. We are further hardening our networks, changing our patching procedures, introducing new vulnerability detection tools, and strengthening our accountability mechanisms.

Fourth, we have committed to working with the entire industry to develop solutions to the growing cybersecurity and data protection challenges we all face.

And, finally, we promised to launch a new easy-to-use app in January that will give consumers the power to lock and unlock access to personal credit data, for free, and for life.

I am pleased to report that we are on schedule with the development of the app, and we are confident consumers will find it extremely valuable.

We have done a lot in a short period of time, but this is just the beginning. I remind my team every day that there are no shortcuts. Strengthening the company's security capabilities and serving consumers requires both a daily engagement and a long-term commitment. And I pledge this is now how we will continue to proceed.

Equifax is made up of 10,000 talented and dedicated people. Our business is not well understood, but it is essential for the economy and for helping consumers obtain the credit they need. Our top job must be to protect the data entrusted to us. We did not meet the public's expectations, and now it's up to us to prove that we can regain their trust.

We are committed to working with consumers, customers, Congress, and regulators to remedy these issues and restore public trust. This has been my focus during my first 6 weeks as CEO, and it will continue to be my focus every day I am in this job.

Thank you for your attention. I welcome your questions.

[The prepared statement of Mr. Barros follows:]

PREPARED STATEMENT OF PAULINO DO REGO BARROS, JR.,
INTERIM CHIEF EXECUTIVE OFFICER, EQUIFAX

Chairman Thune, Ranking Member Nelson, Members of the Committee, thank you for having me here today. My name is Paulino do Rego Barros, Jr. Six weeks ago, I was named interim Chief Executive Officer of Equifax. I never expected to become CEO in these circumstances. But I am honored to have this opportunity to help. Speaking for everyone at Equifax, we are determined to address all the issues from the data breach so that we can regain the confidence of the American people.

Although Equifax is based in Atlanta, I think you can tell from my accent that I did not grow up in Georgia. I am a native of Brazil. I have had the privilege of working most of my adult life in the United States, and my children were born here. In my heart, I have grown to appreciate all that the American way of life and doing business represents—especially when it comes to respect for the consumer.

We have provided the Committee with the summary that Mandiant provided at the conclusion of its forensic investigation. Mr. Smith testified about the details of the breach in prior hearings, and we have briefed Congressional staff about the incident. My focus today will be on our steps going forward as a company, not on the forensic details of the breach.

I am an engineer by training. I have spent a lifetime confronting and fixing complex business problems. This is the mindset I bring to my new position. My first act as CEO was to immediately address the consumer call centers and website. Our initial engagement with consumers was not acceptable. We are working hard to fix these problems.

In an Op-Ed in the *Wall Street Journal,* published on my third day as CEO, I acknowledged that we let down U.S. consumers, our customers, and even our families and friends. I apologized to the American people, and I want to emphasize again to all those who have been affected by the breach how deeply sorry I am. I wish I could turn back the clock to prevent all of this from happening, but I can't. What I promise each of you, and the American people, is that Equifax will be focused every day on strengthening security and providing better support for consumers. We will be an industry leader in giving consumers more control over personal credit data.

In advance of your questions, I would like to review briefly some of the actions we have taken in the past six weeks.

First, my highest priority has been to improve service for consumers. To this end, I have visited call centers, spoken with call center representatives, personally taken calls from consumers, and helped resolve consumer issues. Through social media, we have expanded communications with consumers. Most significantly, we have improved the usability of the website, added staff to the call centers, made the overall experience more consumer-friendly, and substantially reduced delays and backlogs.

Second, we have revised our corporate structure. The Chief Security Officer now reports directly to me, ensuring greater accountability over this critical function. I have also appointed a Chief Transformation Officer to oversee the company's response to the cybersecurity incident and coordinate our efforts to build a new future. This will allow me to have direct insight into every aspect of our remediation efforts.

Third, we are rapidly improving our data security infrastructure. We are further hardening our networks, changing our procedures to require "closed loop" confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. We have also engaged PwC to assist us with our security program, including strategic remediation and transformation initiatives that will help us identify and implement solutions to strengthen our long-term data protection and cybersecurity posture.

We are also working to reinforce the culture of security throughout the entire company. Security is the responsibility of all Equifax employees, whether or not they are members of our Security or Information Technology teams. Since taking this position, I have spoken to our employees at multiple town hall meetings about the absolute necessity of good security practices and the critical importance of protecting consumer information.

Fourth, we have committed to working with the entire industry to develop solutions to the growing cybersecurity and data protection challenges we all face. We see this breach as a turning point—not just for Equifax, but for everyone interested in protecting personal data.

Finally, we promised to launch a new easy-to-use app in January that will give consumers the power to lock and unlock access to personal credit data—for free, for life. I am pleased to report that we are on schedule with the development of the app, and we are confident consumers will find it extremely valuable.

We have done a lot in a short period of time, but this is just a start. I remind my team every day that there are no shortcuts. Strengthening the company's security capabilities and serving consumers requires both a daily engagement and a long-term commitment. I pledge this is how we will continue to proceed.

When I was offered the position, I understood the magnitude of this challenge, but I also recognized an opportunity to give back to the company and this country. Some of my family and friends thought I was crazy for accepting the challenge. Some of you may think the same. I understand. Although the task ahead of us is difficult, I believe that my prior training and years of experience have prepared me well for this job.

Before I close, I want to express my personal appreciation to Rick Smith. Through this challenging transition, he has been fully supportive, as I knew he would be. His contributions to the company have been significant, and I am grateful for his service.

Equifax is made up of 10,000 talented and dedicated people. Our business is not well understood, but it is essential for the economy and for helping consumers obtain the credit they need. Because of our industry, consumers are able to obtain loans for homes, cars, education, and other vital needs. Our business plays an important role in the economy, and our top job must be to protect the data entrusted to us. We did not meet the public's expectations, and now it is up to us to prove that we can be trusted again. We are committed to working with consumers, customers, Congress, and regulators to remedy these issues and restore public trust. This has been my focus during my first six weeks as CEO. It will continue to be my focus every day I am in this job.

Thank you for your attention. I welcome your questions.

The CHAIRMAN. Thank you, Mr. Barros.

Mr. Smith.

STATEMENT OF RICHARD F. SMITH, FORMER CHAIRMAN AND CHIEF EXECUTIVE OFFICER, EQUIFAX, INC.

Mr. SMITH. Thank you. Thank you, Chairman Thune, Ranking Member Nelson, and the honorable members of the Committee. I thank you for the opportunity to testify before you today. I submitted my written testimony to this Committee as well as to a number of other committees in both the Senate and the House I have testified before over the past 3 or 4 weeks. That written testimony is the record of the events of the breach that Equifax incurred, and I'm here today, Mr. Chairman, to answer any questions you may have. Thank you.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF RICHARD F. SMITH, FORMER CHAIRMAN AND CHIEF EXECUTIVE OFFICER, EQUIFAX, INC.

Chairman Thune, Ranking Member Nelson, and Honorable Members of the Committee, thank you for the opportunity to testify before you today.

I was honored to serve as the Chairman and Chief Executive Officer of Equifax for 12 years, until I retired on September 25. As I have previously testified before other Committees of the United States Senate, and before House panels as well, as CEO I was ultimately responsible for what happened on my watch. Equifax was entrusted with Americans' private data and we let them down. For that, I remain deeply sorry. We now know that criminals executed a major cyberattack on Equifax, hacked into our data, and were able to access information for over 145 million American consumers. The information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers; credit card information for approximately 209,000 consumers was also stolen, as well as certain dispute documents with personally identifying information for approximately 182,000 consumers. I want to again express my apologies to everyone affected by this breach.

When we first learned of suspicious activity, I and many others at Equifax worked with outside experts to understand what had occurred and do everything possible to make this right. Ultimately we realized we had been the victim of a massive theft, and we set out to notify American consumers, protect against increased attacks, and remediate and protect against harm to consumers. We developed a robust package of remedial protections for each and every American consumer—not just those affected by the breach—to protect their credit information. The relief package includes: (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft; and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all Americans. We have also taken steps to better protect consumer data moving forward. Equifax also announced a new service that I understand will be available by January 31, 2018, that will allow consumers to control their own

credit data, by allowing them to lock and unlock their credit files at will, repeatedly, for free, for life. This puts the control of consumers' credit information where it belongs—with the consumer. I was pleased to see the company move forward with this plan, which we had put in motion months ago, and which I directed the company to accelerate, as we were constructing the remedial package in response to the breach.

I previously testified in detail about how the breach occurred and what I and Equifax knew and did at specific points in time as this episode unfolded. I would of course be happy to provide the Committee with that detailed information if helpful. I understand that the FBI's investigation and Equifax's own review and remediation are ongoing, as are, of course, numerous other investigations.

Where do we go from here? As you consider the public policy implications of these breaches, two observations occur to me. First, an industry standard placing control of access to consumers' credit data in the hands of the consumers should be adopted. Equifax's free lifetime lock program will allow consumers, and consumers alone, to decide when their credit information may be accessed. This should become the industry standard. Second, we should consider the creation of a public-private partnership to begin a dialogue on replacing the Social Security Number as the touchstone for identity verification in this country. It is time to have identity verification procedures that match the technological age in which we live.

The list of companies and government agencies that have suffered major hacks at the hands of sophisticated cybercriminals is sadly very long, and growing. I was deeply disappointed when Equifax was added to that list. I stepped away from a company I led and loved and helped build for more than a decade. But I remain strongly committed to helping address the important questions this episode has raised. Part of that continues today, as I have previously voluntarily appeared and appear today at this hearing voluntarily to share what I know. Going forward, government and the private sector need to grapple with an environment where data breaches will occur. Giving consumers more control of their data is a start, but is not a full solution in a world where the threats are always evolving. I am hopeful there will be careful consideration of this changing landscape by both policymakers and the credit reporting industry.

Equifax was founded 118 years ago and now serves as one of the largest sources of consumer and commercial information in the world. That information helps people make business and personal financial decisions in a more timely and accurate way. Behind the scenes, millions of Americans have accessed credit, whether to buy a house or a car, pay for college, or start a small business, because of the services offered by Equifax. During my time at the company, working together with our employees, customers, and others, we saw the company grow from approximately 4,000 employees to almost 10,000. Some of my proudest accomplishments are the efforts we undertook to build credit models that allowed and continue to allow many unbanked Americans outside the financial mainstream to access credit in ways they previously could not have. I remain deeply grateful for the 12 years I spent leading the company.

The hard work of regaining the trust of the American people that was developed over the course of the company's history is ongoing and must be sustained. I believe the company, under the leadership of Lead Director Mark Feidler, and interim CEO Paulino do Rego Barros, Jr., will continue these efforts with vigor and commitment.

Chairman Thune, Ranking Member Nelson, and Honorable Members of the Committee, thank you again for inviting me to speak with you today. This was a very difficult experience for the men and women of Equifax but I am confident that under the leadership of Paulino and Mark the company will work tirelessly to regain the trust of American consumers. I look forward to answering your questions and assisting you in any way I can.

The CHAIRMAN. Thank you, Mr. Smith.

Ms. Mayer.

STATEMENT OF MARISSA MAYER,
FORMER CHIEF EXECUTIVE OFFICER, YAHOO!, INC.

Ms. MAYER. Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee, thank you for the opportunity to appear before you today.

I had the honor and privilege of serving as Yahoo!'s Chief Executive Officer from July 2012 through the sale of its core operating

business in June of this year. As you know, Yahoo! was the victim of criminal state-sponsored attacks on its systems, resulting in the theft of certain user information. We worked hard over the years to earn our users' trust. As CEO, these thefts occurred during my tenure, and I want to sincerely apologize to each and every one of our users.

When Yahoo! learned of the state-sponsored attack on its systems in late 2014, Yahoo! promptly reported it to law enforcement and notified the users understood at that time to have been directly impacted. Yahoo! worked closely with law enforcement, including the FBI, who were ultimately able to identify and expose the hackers responsible for these attacks. We now know that Russian intelligence officers and state-sponsored hackers were responsible for highly complex and sophisticated attacks on Yahoo!'s systems. The Department of Justice and FBI announced a 47-count indictment charging four individuals with these crimes against Yahoo! and its users. The DOJ and FBI praised Yahoo! for our extensive cooperation and early proactive engagement with law enforcement.

In November 2016, law enforcement provided Yahoo! with data files that a third party claimed contained Yahoo! user data. Yahoo! determined that user data was mostly likely stolen from the company in August 2013. Although Yahoo! and its outside forensic experts were unable to identify the intrusion associated with the August 2013 theft, the company promptly disclosed the incident, notified the users believed to have been affected, and took steps to secure all user accounts.

I want to stress how seriously I view the threat of cyber attacks and how personally I feel about these potential risks. After growing up in Wisconsin, I remember buying my first computer in college, developing a passion for computer science and writing code, and seeing the potential for how this emerging technology could change the world. After college, I was hired by a small startup named Google, as their 20th employee and first woman engineer. There, over the next 13 years, I worked my way up from software engineer to ultimately becoming a member of the executive operating committee.

In July 2012, I became the CEO of Yahoo! I will always be grateful for and humbled by the opportunity to have led Yahoo! and its employees for the last five years. My experiences from Yahoo! and Google have shown me the amazing potential of the Internet to change our world for the better. They, however, have also reinforced the potential dangers posed by cyber crime.

I am here today to discuss with the Committee, as best I am able, our efforts to confront the challenges of cybersecurity, including some of the security measures and defenses Yahoo! had in place in the hopes of further advancing consumer protection and security.

Throughout my tenure as CEO, we worked hard from the top down and bottom up to protect our systems and our users. We devoted substantial resources to security with a shared goal of staying ahead of the sophisticated and constantly evolving threats. After I joined Yahoo!, we roughly doubled our internal security

staff and made significant investments in its leadership and the team.

In addition to improving our talent, we also improved our security processes and system defenses. Yahoo! had in place multiple layers of sophisticated protection. During my tenure at Yahoo!, we were extremely committed to security and invested tremendous resources. I want to thank all of our team members for their tireless efforts in addressing Yahoo!'s security.

Unfortunately, while all of our measures helped Yahoo! successfully defend against the barrage of attacks by both private and state-sponsored hackers, Russian agents intruded on our systems. The threat from state-sponsored attacks has changed the playing field so dramatically that today I believe all companies, even the most well-defended ones, could fall victim to these crimes.

I will close by saying that cybersecurity is a global challenge. As we have all witnessed, no company, individual, or even government agency is immune from these threats. The attacks on Yahoo! demonstrate that strong collaboration between the public and private sectors is essential in the fight against cyber crime. In addition, aggressive pursuit of cyber criminals, as the DOJ and FBI exhibited in Yahoo!'s case, could be a meaningful deterrent in preventing future crimes like these.

To echo the words of the then Acting Assistant Attorney General overseeing the investigation of the cyber crime perpetrated against Yahoo!: a nation-state attack is not a fair fight, and it is not a fight you will win alone. By working together, we can help to level the cyber playing field.

Thank you for the opportunity to address the Committee today.

[The prepared statement of Ms. Mayer follows:]

PREPARED STATEMENT OF MARISSA MAYER, FORMER CHIEF EXECUTIVE OFFICER, YAHOO!, INC.

Chairman Thune, Ranking Member Nelson, and distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss important issues surrounding consumer protection and data security.

I had the honor and privilege of serving as Yahoo's Chief Executive Officer from July 2012 through the sale of its core operating business in June of this year. As you know, Yahoo was the victim of criminal state-sponsored attacks on its systems resulting in the theft of certain user information. First and foremost, I want to reiterate how sorry I am for these incidents. We worked hard over the years to earn our users' trust, and we fought hard to preserve it. As CEO, these thefts occurred during my tenure, and I want to sincerely apologize to each and every one of our users.

When Yahoo learned of a state-sponsored attack on its systems in late 2014, Yahoo promptly reported it to law enforcement and notified the users understood at that time to have been directly impacted. Yahoo worked closely with law enforcement, including the Federal Bureau of Investigation ("FBI"), who were ultimately able to identify and expose the hackers responsible for the attacks. We now know that Russian intelligence officers and state-sponsored hackers were responsible for highly complex and sophisticated attacks on Yahoo's systems. On March 15, 2017, the U.S. Department of Justice ("DOJ") and FBI announced a 47-count indictment charging four individuals with these crimes against Yahoo and its users. In connection with the government's investigation, the DOJ and FBI praised Yahoo for our extensive cooperation and "early, proactive engagement" with law enforcement, as well as our "leadership and courage," and described Yahoo as "great partners" in the government's multi-year investigation.

As part of our cooperation with the government to try to prevent these type of crimes, in November 2016, law enforcement provided Yahoo with data files that a third party claimed contained Yahoo user data. Yahoo worked closely with law en-

forcement and leading forensic experts to investigate and analyze that data. Following the investigation, Yahoo determined that user data was most likely stolen from the company in August 2013. Although Yahoo and its outside forensic experts were unable to identify the intrusion associated with the August 2013 theft, the company promptly disclosed the incident, notified users believed to have been affected, and took steps to secure all user accounts, including by requiring potentially affected users to change passwords.

The stolen account information included names, e-mail addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers. The stolen account information did not include unprotected passwords, social security numbers, or sensitive financial information, such as payment card data or bank account information.

Before I go on, I want to stress how seriously I view the threat of cyber attacks, and in particular state-sponsored attacks, such as those that victimized Yahoo and its users, and how personally and deeply I feel about these potential risks. After growing up in Wausau, Wisconsin, I remember buying my first computer in college, developing a passion for computer science and writing code, and seeing the potential for how this emerging technology could change the world. After college, my commitment to this field only grew after I was hired by a small start-up named Google as their 20th employee and first woman engineer. There, over the next 13 years, I worked my way up from software engineer to Vice President of Search Products and User Experience, ultimately becoming a member of the executive operating committee.

In July of 2012, I became the CEO of Yahoo. As a pioneer of the World Wide Web, Yahoo was founded in 1994 as the hobby of two Stanford University students and over the next 20 years, Yahoo grew into one of only three Internet companies in the world with more than one billion monthly users. Yahoo is a guide to digital information discovery, focused on informing, connecting, and entertaining users through its search, communications, and digital content products. I will always be grateful for, and humbled by, the opportunity to have led Yahoo and its employees for the last five years.

My experiences from Yahoo and Google have shown me the amazing potential of the Internet to change our world for the better. They, however, have also reinforced the potential dangers posed by cyber crime.

With an increasingly connected world also comes a new host of challenges, including a dramatic rise in the frequency, severity, and sophistication of hacking, especially by state-sponsored actors. I am here today to discuss with the Committee, as best I am able, our efforts to confront the challenges of cybersecurity, including some of the security measures and defenses Yahoo had in place, in the hope of further advancing consumer protection and security. Please understand that the investigations regarding the Yahoo attacks remain active and ongoing, and there are limits on what I know and can discuss about the specific security events. Investigations into data security incidents often evolve over time and my statements today are based on, and limited to, information from my time at Yahoo.

Throughout my tenure as CEO, we took our obligations to our users and their security extremely seriously. We worked hard from the top down and bottom up to protect our systems and our users. We devoted substantial resources to security—both offensively and defensively—with the shared goal of staying ahead of these sophisticated and constantly evolving threats. After I joined Yahoo, we roughly doubled our internal security staff and made significant investments in its leadership and the team. We hired strategically, filling our ranks with security specialists who focused on threat investigations, e-crimes, product security, risk management, and offensive engineering.

In addition to improving our talent, we also improved our security processes and systems defenses. Yahoo's security investments and initiatives included the adoption of a comprehensive information security program that enhanced our policies, procedures, and controls. Yahoo focused its program on the core National Institute of Standards and Technology Cybersecurity Framework functions: identify, protect, detect, respond, and recover.

Yahoo had in place multiple layers of sophisticated protection. Through cross-company initiatives like SSL and HTTPS end-to-end encryption, Account Key and multi-factor authentication, and password hashing and salting protections, Yahoo also helped bolster the company's security defenses and protect its users.

Recognizing that the best defense begins with a strong offense, Yahoo also adopted an attacker-centric approach to its information security program. For example, Yahoo staffed independent teams of some of the world's most sophisticated hackers to proactively attack our systems and report any vulnerabilities. Yahoo also formalized a "bug bounty" program, whereby the company pays security researchers who

report vulnerabilities to the company. Since its inception, Yahoo's bug bounty program helped enhance and harden the security of our products. The bounties awarded by the company surpassed $2 million, with more than 2,500 security researchers participating worldwide.

During my tenure at Yahoo, we were extremely committed to our security programs and initiatives and invested tremendous resources in them. I want to thank all of our team members for their tireless efforts in addressing Yahoo security. As CEO, working with them over the past five years was nothing short of a privilege.

Unfortunately, while all our measures helped Yahoo successfully defend against the barrage of attacks by both private and state-sponsored hackers, Russian agents intruded on our systems and stole our users' data. The threat from state-sponsored attacks has changed the playing field so dramatically that today I believe that all companies, even the most-well-defended ones, could fall victim to these crimes.

I will close by saying that cybersecurity is a global challenge where the security threats, attacks, and techniques continually evolve. As we all have witnessed: no company, individual, or even government agency is immune from these threats. The attacks on Yahoo demonstrate that strong collaboration between the public and private sectors is essential in the fight against cyber crime. In addition, aggressive pursuit of cyber criminals, as the DOJ and FBI exhibited in Yahoo's case, could be a meaningful deterrent in preventing future crimes like these.

To echo the words of the then Acting Assistant Attorney General overseeing the investigation of the cyber crime perpetrated against Yahoo: a nation-state attack is not a fair fight, and it is not a fight you will win alone. By working together, we can help level the cyber playing field.

Thank you for the opportunity to address the Committee today. I look forward to your questions.

The CHAIRMAN. Thank you, Ms. Mayer.

Ms. Zacharia.

STATEMENT OF KAREN ZACHARIA, CHIEF PRIVACY OFFICER, VERIZON COMMUNICATIONS INCORPORATED

Ms. ZACHARIA. Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for the opportunity to testify here today. My name is Karen Zacharia, and I am Verizon's Chief Privacy Officer.

Verizon has a significant and long-standing commitment to protecting and safeguarding consumer data and building trust online. In an increasingly connected world, Verizon recognizes that strong security and consumer trust are prerequisites to compete in the 21st century digital economy. The very nature of our business has always required that Verizon make data security a top priority.

On July 25, 2016, Verizon announced that it had entered into an agreement to acquire Yahoo!'s operating business. That acquisition closed on June 13, 2017. Yahoo! is now part of a new company formed by Verizon called Oath. Oath consists of more than 50 digital and mobile brands globally, including HuffPost, Yahoo! News, Yahoo! Sports, Tumblr, and AOL.

In September and December 2016, Yahoo! announced that certain user data was stolen in two separate incidents in 2013 and 2014. These incidents happened well before Verizon's acquisition of Yahoo!. At the time of the December 2016 announcement, Yahoo! disclosed that more than 1 billion of the approximately 3 billion accounts existing in 2013 had likely been impacted.

After Verizon acquired Yahoo!, we obtained new information from a third party and reviewed it with the assistance of the same outside forensic experts that Yahoo! had used previously. Based on that review, we concluded that all accounts, and not just a subset, were impacted by the 2013 security incident. Yahoo! then provided

further individual notices to the impacted users beginning on October 3, 2017, less than a week after we determined the scope of the impacted user accounts.

In addition, the review confirmed that the stolen information did not include Social Security numbers. It also did not include passwords and clear text. And it did not include sensitive financial information like payment card data or bank account information.

Although Verizon did not own Yahoo!'s operating business at the time of the 2013 data theft or during Yahoo!'s incident response, we understood that Yahoo! took actions around the time of its announcements to protect its users' accounts. Yahoo! required password changes for user accounts where passwords had not been changed since 2014. Yahoo! also invalidated unencrypted security questions and answers so that they could not be used to access an account. Yahoo! took these actions on user accounts beyond those thought to have been impacted by the security incidents. This means that Yahoo! took steps in 2016 to protect all users, including the additional user accounts that were individually notified in October 2017.

Proactively enhancing our security is a top priority at Verizon and Oath. We carefully track the evolution of attacks, gather intelligence, leverage technology advances to make improvements to our systems, and to apply more advanced protection to our user accounts. As part of integrating Yahoo! and AOL into Oath, we are combining two strong existing security teams. We are examining the practices and tools of each team, and applying the best practices and tools across Oath.

We are also in the process of creating an advisory board that will consist of external security experts. The board will provide input to Oath on its overall approach to security. Security has always been in Verizon's DNA, and we remain committed to continuous improvement to meet the security challenges of the future.

At Verizon and Oath, we are laser-focused on the needs of our customers. We know that they expect that their information will be secure. As a result, we go to great lengths to integrate security across our networks, platforms, and products. We are committing substantial resources to defend our company's assets, networks, and customers, including those acquired with the closing of the Yahoo! transaction.

With the benefit of Verizon's experience and resources, along with a commitment to the highest level of accountability, Verizon and Oath will continue to strive to stay ahead of an ever-evolving threat landscape.

Thank you again for the opportunity to testify today. I look forward to answering your questions.

[The prepared statement of Ms. Zacharia follows:]

PREPARED STATEMENT OF KAREN ZACHARIA, CHIEF PRIVACY OFFICER, VERIZON COMMUNICATIONS INCORPORATED

Chairman Thune, Ranking Member Nelson, and Members of the Committee, thank you for the opportunity to testify.

Witness Biography

My name is Karen Zacharia. I am Verizon's Chief Privacy Officer and I lead the Privacy Office, a centralized department responsible for privacy and data security

compliance. My team provides its expertise across the company so that throughout the lifecycle of our products and services we are addressing privacy and data security every step of the way. We maintain and update Verizon's privacy policies, counsel on internal and external privacy principles and requirements, and provide training to employees on existing and new privacy laws and Verizon policies. My office also spends a significant amount of time focusing on core privacy commitments like transparency and choice so that our customers can make meaningful choices when it comes to their personal information.

Verizon/Oath/Yahoo Background

Verizon has a significant and longstanding commitment to protecting and safeguarding consumer data and building trust online. In an increasingly connected world, Verizon recognizes that strong security and consumer trust are prerequisites to compete in the 21st Century digital economy. The very nature of our business has always required that Verizon make data security a top priority.

On July 25, 2016, Verizon announced that it had entered into an agreement to acquire Yahoo's operating business. That acquisition closed on June 13, 2017. Yahoo is now part of a new company formed by Verizon called Oath. Oath consists of more than 50 digital and mobile brands globally, including HuffPost, Yahoo News, Yahoo Sports, Tumblr and AOL.

2013 and 2014 Yahoo Security Incidents

In September and December of 2016, Yahoo announced that certain user data was stolen in two separate incidents in 2013 and 2014. These incidents happened well before Verizon's acquisition of Yahoo.

At the time of the December 2016 announcement, Yahoo disclosed that more than one billion of the approximately three billion accounts existing in 2013 had likely been impacted. After Verizon acquired Yahoo, we obtained new information from a third party and reviewed it with the assistance of the same outside forensic experts that Yahoo had used previously. Based on that review, we concluded that all accounts—and not just a subset—were impacted by the 2013 security incident. Yahoo then provided further individual notices to the impacted users beginning on October 3, 2017—less than a week after we determined the scope of the impacted user accounts.

In addition, the review confirmed that the stolen information did *not* include Social Security numbers. It also did *not* include passwords in clear text. And it did *not* include sensitive financial information like payment card data, or bank account information.

Although Verizon did not own Yahoo's operating business at the time of the 2013 data theft or during Yahoo's incident response, we understand that Yahoo took actions around the time of its announcements to protect its users' accounts. Yahoo required password changes for user accounts where passwords had not been changed since 2014. Yahoo also invalidated unencrypted security questions and answers so that they could not be used to access an account. Yahoo took these actions on user accounts beyond those thought to have been impacted by the security incidents. This means that Yahoo took steps in 2016 to protect all users, including the additional user accounts that had been individually notified in October 2017.

Verizon's Focus Following Acquisition of Yahoo

Proactively enhancing our security is a top priority at Verizon and Oath. We carefully track the evolution of attacks, gather intelligence, and leverage technology advances to make improvements to our systems and to apply more advanced protection to our users' accounts.

As part of integrating Yahoo and AOL into Oath, we are combining two strong, existing security teams. We are examining the practices and tools of each team, and applying the best practices and tools across Oath. We are also in the process of creating an advisory board that will consist of external security experts. This board will provide input to Oath on its overall approach to security.

Security has always been in Verizon's DNA and we remain committed to continuous improvement to meet the security challenges of the future.

Conclusion

At Verizon and Oath, we are laser-focused on the needs of our customers. We know that they expect that their information will be secure. As a result, we go to great lengths to integrate security across our networks, platforms, and products. We are committing substantial resources to defend our company's assets, networks, and customers, including those acquired with the closing of the Yahoo transaction.

With the benefit of Verizon's experience and resources, along with a commitment to the highest level of accountability, Verizon and Oath will continue to strive to stay ahead of an ever-evolving threat landscape.

Thank you again for the opportunity to testify today. I look forward to answering your questions.

The CHAIRMAN. Thanks, Ms. Zacharia.

Mr. Wilkinson.

STATEMENT OF TODD WILKINSON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ENTRUST DATACARD

Mr. WILKINSON. Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for the opportunity to discuss the recent major data breaches that have touched the vast majority of American consumers and the urgent actions necessary to protect sensitive personal information.

For almost 50 years, Entrust Datacard has provided solutions that enable the creation of secure physical and digital identities that are used around the world in banking, government, and enterprise applications. Identity is a foundational element of our commerce system and the way Americans build their financial lives. The value of identity is the primary reason this information is targeted and why we continue to see more sophisticated attacks that lead to significant data breaches.

We live in an incredibly connected and complex world. The challenge of protecting data is an evolving and sophisticated task, but it starts with a secure identity. This will only become more critical as we continue to drive toward greater connectivity, linking virtually every aspect of our lives to a connected system.

According to the 2017 Verizon Data Breach Investigations Report, 43 percent of all data breaches can be traced to a phishing attack in which a malicious actor was able to compromise an identity and use this information to gain access to data. Once compromised, a primary target is consumer identities. The information stolen in the most recent breaches contained a significant amount of personally identifiable information, or PII, belonging to millions of American citizens. The focus of this hearing is to examine the recent data breach events, identify steps that could have been taken to ensure the safety of consumer data, and to determine if there are options to further safeguard consumer identities in the future.

Regarding the issue of steps that can be taken to better ensure the safety of consumer data, today organizations are challenged by increasingly complex systems and arising attacks from nation-states and other well-organized groups. This Committee can bring forward a number of experts. Most will agree that no system is free from vulnerabilities, and all have the potential to be breached. However, there are documented best practices and numerous security tools available to mitigate common attacks, and the vast majority of major breaches are still the result of common security mistakes and stolen credentials resulting from poor cyber hygiene.

Today, a substantial amount of PII that is the basis of our identities used for secure transactions has already been stolen and can potentially be used to defraud consumers. It is essential to now find a balance between driving responsible behavior in enterprise

security and providing an answer to the underlying security of consumer identities. To address consumer identity, it will be critical to implement a resilient identity system that can respond to compromise with the ability to recover quickly and to ensure consumer data is no longer at risk.

Today, the Federal Government provides a nine-digit number issued on a paper card, our Social Security card. This static number is generally issued at birth and difficult to change without significant inconvenience to the citizen.

While we have made significant advances in technology, this foundational form of identification has not changed, leaving consumers vulnerable to compromise. Our recommendation to this Committee is that the time is upon us to create a new identity framework. This new framework would create a modern secure identity through a collaboration of government and industry.

There are several examples of public-private partnerships around the world delivering stronger identity frameworks as a foundation for commerce. A new identity framework will allow citizens to utilize a more secure method to transact, and to do so in a manner that reduces the potential of breach or compromise. In all use cases, this new identity framework could minimize risk and inconvenience to the consumer in cases of breach, and allow a consumer to more easily recover their identity with minimal impact.

Our identity system today is broken; it is not secure. It is time to leverage available technologies to provide Americans with new mechanisms to protect their identities. In my company's previous testimony, we have recommended the best path forward rests upon a public-private ecosystem that's built upon good security governance, secure identities, and constant self-assessment of vulnerabilities. Whether we drive adoption via incentive or directive, we need to proceed now. I urge you to focus on near-term actions to address the consumer information that has already been compromised while working toward longer-term solutions which create a more resilient identity for American consumers.

Chairperson Thune, Committee members, fellow panelists, thank you for your time today.

[The prepared statement of Mr. Wilkinson follows:]

PREPARED STATEMENT OF TODD WILKINSON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ENTRUST DATACARD

Chairman Thune, Ranking Member Nelson and members of the Committee, thank you for the opportunity to discuss the recent major data breaches that have touched the vast majority of American consumers and the urgent actions necessary to protect sensitive personal information.

For almost 50 years, Entrust Datacard has provided solutions that enable the creation of secure physical and digital identities that are used around the world in banking, government and enterprise applications. Identity is a foundational element of our commerce system and the way Americans build their financial lives. The value of identity is the primary reason this information is targeted and why we continue to see more sophisticated attacks that lead to significant data breaches.

We live in an incredibly connected and complex world. The challenge of protecting data is an evolving and sophisticated task, but it all starts with a secure identity. This will only become more critical as we continue to drive toward greater connectivity, linking virtually every aspect of our lives to a connected system. According to the 2017 Verizon Data Breach Investigations Report, 43 percent of all data breaches can be traced to a phishing attack in which a malicious actor was able to compromise an identity and use this information to gain access to data. Once

compromised, a primary target is consumer identities. The information stolen in the most recent breaches contained a significant amount of personally identifiable information (PII) belonging to millions of American consumers.

The focus of this hearing is to examine the recent data breach events, identify steps that could have been taken to better ensure the safety of consumer data and to determine if there are options to further safeguard consumer PII in the future.

Regarding the issue of steps that can be taken to better ensure the safety of consumer data, there are well documented best practices and numerous security tools available to mitigate common attacks. However, this committee can bring forward a number of experts, and most will agree that no system is free from vulnerabilities and all have the potential to be breached.

Additionally, a substantial amount of PII has already been stolen and can potentially be used to defraud consumers. It is essential to now find a balance between driving responsible behavior in enterprise security and providing an answer to the underlying security of the consumer identity. To address consumer identity, it will be critical to implement a resilient identity system that can respond to compromise, with the ability to quickly recover and to ensure consumer data is no longer at risk.

The State of Identity Today

The implications of using an insecure identity go far beyond that of financial burden or inconvenience to the consumer. The use cases for our government issued identity stretch across all aspects of life, and if compromised, there is no process in place by which citizens can easily reestablish and recover their identity.

Commerce

Over the course of an eligible consumer's life they will engage in a variety of commerce activities that require the completion of an application that includes the public disclosure of their recognized identity—their social security number. From opening a banking account, to applying for a home or auto loan to requesting a new credit card from a big box retailer. While the application may take on a variety of forms—paper, digital and oral—the one thing each application has in common is that the citizen is put at risk of their personal identity credentials being compromised. Paper application documents that are not disposed of properly, or the breach of a digital database are common and easily compromise the consumer's identity. Yet, without the disclosure of the identity credential, a consumer is not be able to establish their identity and is restricted from conducting commerce.

Employment

The social security number was introduced in the 1930s as a means of recording and dispensing funds earned by citizens for retirement. The number was also intended for tax recording purposes.

When applying for employment, or when completing new employment paperwork, employees are required to provide employers with their social security number. Each time a person applies for a position and with each subsequent employment change, the applicant must provide an employer with their social security number.

Recent breaches of employee data have also been reported, exposing the personal information of millions. In June 2015, the Office of Personnel Management (OPM) announced that over 21 million records containing PII, including social security numbers, were stolen.

In the case of the OPM breach, the records compromised were tied to background investigation records, a common practice among many employers today. Many times, new employees are required to submit their identity for review by their employer. Should the identity of an individual be compromised without their prior knowledge, it could be career limiting: a background check of an employee whose identity has been compromised might falsely reveal financial difficulties or criminal histories—causing the applicant to lose the job opportunity and the employer to lose a valuable employee. The breach of personal information can also create the opportunity for bribery or blackmail from criminals or foreign powers that might hone in on those whose personal information reveals financial burdens or compromising information.

Insecure Identity: Risks and Impacts

To better illustrate this point, let's reflect on another major breach that occurred in 2013. In March 2014, one of my staff members at the time, David Wagner, testified in front of this committee in response to a breach of credit and debit card information by a major retailer that affected more than 40 million people. While this breach, and subsequent breaches of payment data, impacted consumers, they were able to quickly address the compromise. This is because the payment ecosystem was designed to be resilient. When fraud occurs, the liability largely falls to the financial

institution not the consumer. In addition, financial cards are easily replaced by new payment credentials, thereby eliminating the risk of fraud on a compromised payment card.

The difference with today's conversation is that the compromised data is not a credit or debit card that can be easily replaced. It is a social security number, a name, an address that can have far reaching and long lasting impacts to those compromised. Over 145 million Americans' insecure identities are now forever at risk, and they have limited ability to protect themselves. A key question for this committee to consider is: What do we do now given these identities are forever compromised? The critical issue to address is the ability to recover from a data breach with a resilient secure identity.

Secure, Modern Identities

To address the challenges brought on by the current pattern of breached insecure identities, we should focus on how to help consumers recover. In today's environment, the only recourse a consumer has is to work with each credit reporting agency to lock their credit, ensuring that it cannot be used or to contract with a credit monitoring service that will do this on behalf of the consumer. The consumer is burdened with the cost and the time it takes to try to protect themselves.

Given most American consumer identities have already been compromised, it is imperative that action is taken to put the consumer back in control of how and when their identity is used. It is our strong recommendation that any use of personal information, whether an account opening, credit requests, transaction attempts, etc. require consumer authorization through a strong authentication mechanism. Putting the consumer in control could be implemented by leveraging the consumer's mobile device, as is common in banking applications today. The technology required for implementation is well tested and works at scale.

A modern secure identity system needs to strike a balance of providing an appropriate level of information to enable commerce activities, while providing consumers with the ability to quickly, and cost effectively, reestablish their identity and then move on with their lives without fear of further repercussions.

Key Characteristics of a Modern Secure Identity: Identity Should Be Dynamic

As already mentioned, today's primary identity source, the social security number, is issued at birth and is difficult to change without significant inconvenience to the citizen. With a dynamic identity, a compromised identity can be revoked and replaced, reducing inconvenience or effort on the part of the citizen.

Dynamic identities are commonplace in Brazil, where Infraestrutura de Chaves Públicas (ICP)—Brasil issues digital certificates (a digital identity) for citizen identification. In this example, the government owns the core identity issuing technology, but partners with industry to provide consumer options for how to access this identity system. These certificates generally last one to three years and can be used to digitally sign documents with the same force as a written signature, access government systems online and provide easier and secure online access to financial institutions. A critical point is that ICP-Brasil has institutionalized the concept of dynamic identities. Even if the identity is not compromised, it still has a relatively short validity period. And in the event of a compromise, the process to replace the identity with a new one is well understood and easily executed.

Identity is Easy to Issue, Revoke and Manage

We must be able to issue an identity (and revoke and re-issue it) without tremendous effort on the part of the user. When an identity is revoked, the revocation must be pervasive so that everyone can easily know what has been revoked and reissued. Payment cards are easily revoked; attempts to pay with a cancelled card are immediately declined.

The Consumer Controls their Identity

When individuals are personally accountable and in control of their own secure identities, they can determine which factors are in place to help confirm their identities. Identity factors are not reliant on data like address, telephone number, mother's maiden name or names of pets—these examples, like social security numbers, are static pieces of information that are easy for someone else to discover. Instead, more sophisticated factors like fingerprints and facial recognition could be used. Other factors, such as behavioral attributes and verifications through a mobile device, are also in wide use. The user can choose to confirm their identity through a variety of factors—a best practice in enterprise security is to use more than one factor. Individuals should have the ability to select which and how many factors to use, giving them control over how they secure and manage their identity.

A New Identity Framework

Our recommendation to this committee is that the time is upon us to create a new identity framework. This new framework would create a modern secure identity through a collaboration between government and industry. In all use cases, this new identity could minimize risk and inconvenience to the consumer in cases of breach, and allow a consumer to more easily recover their identity with minimal impact.

Our identity system today is broken—it is not secure. It is time to leverage available technologies to provide Americans with new mechanisms to protect their identities. In my company's previous testimony, we recommended the best path forward rests upon a private-public ecosystem that is built upon good security governance, secure identities and constant self-assessments of vulnerabilities.

Whether we drive adoption via incentives or directives, we need to proceed now. I urge you to focus on near-term actions to address the consumer information that has already been compromised while working toward long-term solutions which create a more resilient identity.

Chairperson Thune, committee members, fellow panelists—Thank you for your time today.

The CHAIRMAN. Thank you Mr. Wilkinson.

I'm going to start with the questions, and I'll start with Ms. Mayer. In your opening statement, you described the significant investments that Yahoo! made under your leadership with respect to its internal security. Nevertheless, despite these investments, the company apparently failed to detect the 2013 breach, which was the largest breach in the history of the Internet, for more than 3 years. And even after the 2013 breach became apparent, Yahoo! significantly underestimated the number of accounts implicated by billions.

And so I'll give you an opportunity to answer the obvious question, but that is with such a strong security team in place, how did Yahoo! fail to recognize that all 3 billion of its user accounts had been compromised? And why did it take more than 3 years to discover and to disclose the breach?

Ms. MAYER. At Yahoo!, we deeply valued our user security and invested heavily in that security. As is frequently the case in these types of cyber attacks, they are complex, they are persistent, and in often cases, the understanding of the facts evolves over time. To this day, we, as I understand it, still have not been able to identify the intrusion that led to that theft, which is to say we have received files from law enforcement that contained Yahoo! data, and we verified that it came from Yahoo!. We don't exactly understand how the act was perpetrated. And that certainly led to some of the areas where we had gaps in information.

The CHAIRMAN. Why the delay in disclosing it? I mean, it took 3 years. How was it possible to underestimate by billions literally the number of consumers who were impacted by it?

Ms. MAYER. Yahoo! did not know of the intrusion in 2013. We learned of the intrusion by files that were presented to us in November 2016. And in a very short period of time, we verified that that data was taken from Yahoo!, that it was most likely from August 2013, notified law enforcement, notified our users, and took protective actions on all the accounts. And at that time, we estimated that it affected more than 1 billion users. There have been recent announcements from Verizon that I'm not privy to since I'm no longer with the company.

The CHAIRMAN. So the 500 million that was originally disclosed, and then it jumped up to 3 billion, there's no real explanation, at

least to your knowledge, for how you miscalculated the number of people impacted?

Ms. MAYER. The 500 million number was related to the fall 2014 breach by the Russian hackers where the indictments were issued by the DOJ and FBI.

The CHAIRMAN. Mr. Smith, in prior testimony before Congress, you said that the failure to patch a known vulnerability in your system basically boiled down to a single employee's failure to act, compounded by an IT scan that should have detected that failure, but didn't. Then to add insult to injury, the vulnerability was allowed to persist for several months without corrective action being taken.

So for a company that holds some of the most sensitive personal information on millions of American consumers, I hope you can understand why this revelation is so hard to understand. Can you explain why there weren't more trip wires or redundancies built into your system to prevent something like this from happening? You've also testified that these weaknesses have now been addressed, perhaps you could also elaborate on how.

Mr. SMITH. Yes, Mr. Chairman, you're right. In prior testimonies, I refer to the fact that we were notified by U.S. CERT on March 8 of this year, communicated per our protocol on the ninth to patch the vulnerability in the Apache Struts software, open-source software, that existed. The e-mail did go out per our protocol. On the fifteenth of March, we then scanned, and the scanner did not find the vulnerability. So the human errors I described in the past, as well as the technology error, both led to the ability for the criminals to access what we call our web portal dispute environment.

The CHAIRMAN. But why wouldn't you have had more redundancies built into your system? Why did it basically come down to one employee? That seems really hard to fathom for a company that specializes in what you do.

Mr. SMITH. A clarification. Yes, the redundancy was a scanner, and the scanner did not work as well. So you had the human process, which is standard process of identifying a patch, the vulnerability, applying the patch, and then going back a week later with a technology scanner to see if the patch was applied.

The CHAIRMAN. You said you've fixed that or can you elaborate a little bit on that? And maybe Mr. Barros as well could elaborate on any further steps that Equifax has taken since the breach.

Mr. SMITH. I'll start, and Mr. Barros can continue, if you will.

What we had installed shortly after, about the time of one of my last hearings, was a new scanning technology. We upgraded a scanning technology to a new generation scanner that seems to be a better scanner than the prior scanner. There were some process changes Paulino may want to talk about as well.

Mr. BARROS. Sure. As you can imagine, security is my top priority, including strengthening security systems in our company. We have done a comprehensive top-down review of the process with the help of PwC and Mandiant, and we are strengthening all aspects of our operations, including our patching capabilities. We are enhancing and updating our tools to make sure that we have an effective patching system in place. We have actually put stronger policies in place to make sure that we have more redundancies and

closed loops, in order to make sure that our actions will be executed with accuracy.

The CHAIRMAN. Have you disposed of the data that you no longer need? Has Equifax disposed of——

Mr. BARROS. This is part of the process that we're going through right now. We are evaluating the data architecture that we have to have in place.

The CHAIRMAN. How about encrypted?

Mr. BARROS. We are adding whatever is necessary to do it, including encryption, including tokenization, including all new technologies available to make sure that we protect the data, both with respect to the data itself and the architecture of the data.

The CHAIRMAN. Thank you.

Senator Nelson.

Senator NELSON. Ladies and gentlemen, we've had these hearings before, and if we don't do something, we're going to be having these hearings again. At this point, I'm wondering that there is such a thing as data security. When you think of a sophisticated state actor such as China or Russia, your companies can't stand up against them.

The only person or institution that can stand up against state actors is the National Security Agency. And what we're going to see in the future for not only personally identifiable information, but the state secrets of our country, many of which are critical infrastructure, as represented by companies such as yours, is a need for cooperation between the most sophisticated player in the United States, the NSA, and you all.

Otherwise, Americans are not going to have any more privacy. And if we don't do something and if you all don't do something to change this, we're going to be right back here having additional hearings on this same topic.

Ms. Mayer, what do you think? You had a sophisticated state actor coming after you. How do you really think that you could have protected yourself?

Ms. MAYER. Even robust defenses and processes are not sufficient to protect against a state-sponsored attack, especially when it's extremely sophisticated and persistent. We, at Yahoo!, cooperated with law enforcement and brought these breaches and intrusions to the attention of law enforcement swiftly each time they were detected, and the DOJ and FBI were of great assistance to the company in identifying the perpetrators and bringing them to justice.

Senator NELSON. That's an admission that you're not protected against a state actor.

So now, Ms. Zacharia, you all own Yahoo!. What are you all going to do about it?

Ms. ZACHARIA. Thank you, Senator. A couple of different things. First, your point that we have to work together is absolutely right. I think we need to work both with industry and with government to try to tackle this problem. And that's true in a number of different areas. Verizon, for example, has long believed that there should be national data security and data breach legislation, and we would be happy to work with any of the Senators here on what that legislation should look like.

In addition, though, all of our security teams need to understand that security isn't static, it's always changing. The attackers are getting better, the tools are getting better, the intelligence that we're gathering is changing. And so as that's happening, we have to make sure that we're changing our security systems to improve and keep up.

Senator NELSON. That's a good intention, but it's going to take more. It's going to take an attitude change among companies such as yours that you have got to go to extreme limits to protect customers' privacy.

So, Mr. Smith, you hold a financial guillotine over a lot of your customers by virtue of what their credit rating is. So if your data is not protected, and a poor little fellow goes to buy a house, and is ready with the down payment, he may not get a mortgage because he has got a black mark on his credit rating that is not real, but has been placed there because of a data breach, preventing him from closing on his house. This has huge consequences. What are you and Mr. Barros going to do about it?

Mr. SMITH. Mr. Senator, there is no doubt that securing data is the core value of our company. And I will also, like Mr. Barros said, apologize deeply to the American public for the breach that we had. We let the public down.

I'll tell you this, I do agree with the other panelists here, and your point earlier, Mr. Senator, a combination cooperation between public-private to address this issue is needed. In my 12 years of running the company and tracking the velocity, the increase, of cyber attacks is remarkable to see. In prior testimonies, I talked about the fact that it's not unusual for us in any one given year to see suspicious activity, unwarranted attempted attacks, of millions per year.

Senator NELSON. Mr. Smith, didn't you describe Equifax as the victim when the company failed to secure the security vulnerability that led to the breach? Is Equifax really the victim?

Mr. SMITH. I believe I described it as a—we're a victim of a criminal attack.

Senator NELSON. Mr. Wilkinson, do you consider Equifax to be a victim?

Mr. WILKINSON. Senator, I think they are a victim, as my fellow panelists pointed out. Certainly, there have been many victims in the cases of these breaches. But the criminal impact from hackers moving into these enterprises creates them also to be in a position to be a victim, in my opinion.

Senator NELSON. Well, do you believe that they had adequate security measures in place?

Mr. WILKINSON. Based on my understanding of the breach that occurred at Equifax, and we're talking about effectively patching of security vulnerabilities in a timely way, we've heard some discussion of some of the increase in security stance that they've had since the breach. These are the types of things that I would suggest to you are basically understand are best practices. Most security——

Senator NELSON. I don't understand your answer. Do you consider them to have had appropriate security protocols?

Mr. WILKINSON. Having not patched for as long as they did, I would not recommend suggesting that that was adequate security protocol.

Senator NELSON. OK. So the answer is no.

Mr. WILKINSON. No.

Senator NELSON. So Equifax is not the victim, it's the poor customers of Equifax who are victims. Is that correct?

Mr. WILKINSON. Both are—I believe both are victims, Senator, in my opinion.

Senator NELSON. OK. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson.

Senator Wicker.

STATEMENT OF HON. ROGER F. WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Mr. Smith, in your written testimony, one of your suggestions is a public-private partnership to begin a dialogue on replacing Social Security numbers as methods of verification. I wonder if your suggestion would also apply to rethinking the use of passwords and user ID numbers.

And I'm going to ask Mr. Wilkinson to address this question also because in your testimony, Mr. Wilkinson, you talk about dynamic identities as a way to replace the Social Security number in the modern age, and you point to Brazil as a better example where the government owns core identity issuing technology and issues some sort of digital identity that might last for 3 years.

So I'll go to Mr. Wilkinson first and then back to Mr. Smith. Is that system working better for the consumer in Brazil, or is it just a helpful aspect, but it still doesn't get the job done against this onslaught which Senator Nelson described in his question?

Mr. WILKINSON. Thank you for the question, Senator. There were two questions. In the beginning, in your first question, you asked the question about the use of passwords and, you know, identifiers, as well as Social Security number. With static information, like username password or Social Security number, you have a generally weak identity framework, which is why we talk about the need for additional security.

Now, there are many tools today that many companies are using around secure authentication that help overcome some of the vulnerabilities that we see from things like username passwords. Some of those tools need to be deployed as we talk about where we use Social Security numbers as a primary form of our identification that forms the basis of our identity.

In my written testimony, I also provided some additional examples of what we see other countries doing that I won't suggest to you are best practices, but I would suggest would be important for this Committee to look at. In some cases, these countries have moved to digital identity systems, in part because they didn't have anything in place.

What our recommendation is, of course, we've moving from a system that's worked in the United States for probably 50 years but no longer is secure. The example that you cite from Brazil is a form of digital identity that is issued by the Federal Government for the

purpose of providing a citizen with a digital identity that they can use for certain transactions, high-security needs, digital signing requirements, and has a limited life, in that case, 3 to 5 years. So the combination of the way that they have deployed that identity framework is more secure and provides the ability to be more resilient than what we see today, and what we're able to recover from in the event of a breach like what we just talked about from Equifax.

Senator WICKER. In your view, the consumer is better protected under this Brazilian system?

Mr. WILKINSON. They can be, yes.

Senator WICKER. Mr. Smith, what do you say?

Mr. SMITH. I would agree. And not much I can add to that, but the concept of using a static 1936 instrument like the SSN and thinking it's secure, we've outlived that concept. Some combination of digital multifactor authentication, as Mr. Wilkinson talked about, I think is the right path.

Senator WICKER. Ms. Zacharia, you suggest legislation, and it might be that all five members of the panel are advocating legislation. We only have one minute and 23 seconds left, but in general, what would this legislation look like?

Ms. ZACHARIA. I think the two key things that should be in data breach legislation are, number one, that it be a national framework so that we have one standard to comply with as we're responding to a data breach; and, number two, it's really important that it get the standard right for when we notify customers. It's important to notify customers about information that they really need, but to make sure that we're not notifying them so often about so many things that they stop paying attention.

Senator WICKER. And would anyone like to take issue with Senator Nelson's overall conclusion that really against a state actor like we've seen, a mere company is just unable to withstand that without going to NSA? Does anybody want to disagree with that?

[No audible response.]

Senator WICKER. No takers.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Wicker.

Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you for having this hearing.

Thank you to the witnesses for being here today.

I think almost every American consumer at this point is aware of the unacceptable risks that right now are entailed in many of our business practices, risks to their privacy information that they expect and reasonably anticipate will be safeguarded by companies that do business with them and where they are customers.

The Equifax breach, in particular, exposed the limits of the Federal Trade Commission's ability to protect consumers and impose civil penalties on companies that treat our data with negligence and recklessness. Under current law, even some of the most egregious examples of lax security can be met only with apologies and

promises to do better next time, not fines or other penalties for real deterrents that provide incentives to business executives to actually do better. The real deterrent will come when those penalties are imposed on executives, like the ones before us today. And if the entities that hold our data cannot be trusted to protect it, then the government needs to have the tools to not only go after hackers and thieves, but also hold companies accountable.

Commonsense legislation I have introduced, the Data Breach Accountability and Enforcement Act of 2017, would ensure that the FTC can investigate any data breach by any company or organization that holds sensitive consumer data, including nonprofits, and can impose civil penalties that are actually sufficiently strong to motivate companies to implement strong security at the onset. In this area, truly an ounce of prevention is worth a pound of cure. In fact, in many instances, for many consumers, there is no real cure.

When you were here last, I think it was the last time you were on the Senate side at least, you came before the Judiciary Committee, Mr. Smith, and I asked you whether you could commit that none of your consumers would ever be required to go through arbitration. You said, understandably, that you were no longer with the company, and, therefore, you couldn't guarantee.

So I'm going to ask Mr. Barros, and I appreciate your being here today, I have the same question. Can you guarantee that no consumer will be required to go through arbitration if they decide to use one of your services or products?

Mr. BARROS. Senator, I understand the issue related to the arbitration clause initially included in the TrustedID Premier product when it came out, and it was immediately removed. Arbitration is a tool used by the industry, especially the consumer industry. We have used that tool as permitted by the law. We will continue to evolve in this process and examine the use of this arbitration process——

Senator BLUMENTHAL. And I apologize for interrupting you, but my time is limited, as you understand. So this is one of those yes-or-no answers, I think. Can you guarantee that you won't use arbitration? I understand all of the "on the one hand, on the other hand" comments that could be made. But consumers expect that they will have a right to go to court and have their rights vindicated there. Can you guarantee that you will not force them to use arbitration?

Mr. BARROS. I believe the consumers have a choice to choose the products that they need.

Senator BLUMENTHAL. But if they choose your products, they will not be forced into arbitration. You are guaranteeing that?

Mr. BARROS. We work according to the law and use the tools that the industry uses to have arbitration in place.

Senator BLUMENTHAL. Do you know the difference between a credit freeze and a credit lock?

Mr. BARROS. Yes, I know.

Senator BLUMENTHAL. Can you guarantee that the credit lock, if you use them, will be subject to consumer protection under the state laws where consumers live?

Mr. BARROS. I understand the way we use freeze and lock, at the end of the day for the consumer, it provides the same result. The state law requires a different regulatory process for you to obtain the freeze.

Senator BLUMENTHAL. The difference is credit freezes are regulated by states——

Mr. BARROS. Correct.

Senator BLUMENTHAL.—credit locks are not. You're resorting to credit locks. Is it to avoid state——

Mr. BARROS. No.

Senator BLUMENTHAL.—oversight and scrutiny?

Mr. BARROS. I'm sorry. No, no, not at all. We did it because it's simple to use, it's more accessible to use, and it's easy to understand by the consumer.

Senator BLUMENTHAL. My time has expired. Thank you, Mr. Chairman. I hope we'll have a second round.

The CHAIRMAN. Thank you, Senator Blumenthal.

Senator Schatz.

STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII

Senator SCHATZ. Thank you, Mr. Chairman.

Mr. Barros, thank you for being here. Do you think consumers should be able to see the same information that their bank uses when the bank makes a credit decision?

Mr. BARROS. We have, as an industry, not done a good job representing to the consumer the role we play in this process. The information is provided by the consumer when they are in the process of acquiring a new car, or a credit card. This information is turned over to, usually or most of the time, a financial institution.

Senator SCHATZ. Right. I understand how it works, I'm just saying that when the bank evaluates my creditworthiness, they get a bunch of data. I don't get to see what they're looking at. Do you think I should be able to see what they're looking at when evaluating my creditworthiness?

Mr. BARROS. You——

Senator SCHATZ. This is also probably a yes-or-no answer.

Mr. BARROS. You have access to your credit report. You have access to your score. This is the information that they use, most of the time, to make a decision.

Senator SCHATZ. It's the same information?

Mr. BARROS. A credit report is the same as they have, the same—my credit—my score is the same as they have. So it's information they use to make a decision. They're allowed to see the information.

Senator SCHATZ. You're telling me that the information that a so-called customer has is all that a bank is provided by Equifax?

Mr. BARROS. I don't know. I don't know what the—I don't know what information the bank provides. I know what I provide to the bank.

Senator SCHATZ. Yes, well, Mr. Smith, you sounded like you wanted to correct——

Mr. SMITH. No, no, just if I may add something to it for clarification.

Senator SCHATZ. Sure.

Mr. SMITH. If a consumer is going to a bank to apply for a loan of some sort, typically the underwriter at the bank would pull a credit file, either ours, TU, or Experian. The consumer has the right to get access to that free every year themselves. They also have access to the score, as Mr. Barros said. I think what you're referring to is the banks don't just use a standard score like a FICO score, they may have their own score, and that score is not disclosable to the individual consumer.

Senator SCHATZ. OK. Are we your customers? Are people—the people that—the people whose data was breached, are we your customers, or are the lenders your customers? How do you see that?

Mr. BARROS. Well, a small part of Equifax's business deals directly with consumers, but most of Equifax's customers are institutions that have individual consumers as their customers.

Senator SCHATZ. OK. Because it seems to me that there is actually a line on this, on that side of the dais, which is to say, not to excuse what happened with Yahoo!, but it is different. The incentives are different between the credit reporting agencies, who have essentially zero financial incentive to get it right.

You guys get informed by the Department of Homeland Security that there is a vulnerability. You get provided the patch. You don't download the patch. Your scanner doesn't work. Executives cash out their stock. You then start charging people to lock their credit or freeze their credit. You then start to promote through LifeLock, you have commercials with LifeLock, saying, "Hey, there's been a breach. You might want to use this product." LifeLock subcontracts to Equifax. You guys continue to be profitable.

On the other side, for Verizon, for Yahoo!, for Google, for other companies, if you screw up with your customers, there is a customer relationship that is frayed.

But in the case of the credit reporting agencies, there is no volition on the side of the customers, and that's the foundational problem here, which is that there is no incentive on your side to do anything other than to charge us to solve the problem that you caused, there is no incentive on your side to spend the money that it would take to transform the company to actually treat us like customers because your customers are lenders, your customers are not the people who got harmed through the breach.

Mr. Barros, do you want to respond to that?

Mr. BARROS. I think that the biggest incentive that we have is the stewardship that we have, the obligation that we have with the consumers to keep their data accurate and safe.

Senator SCHATZ. Right, but that's not a fiduciary. I mean, you have an earnings call I think tomorrow or shortly, and you're going to report presumably that everything is fine or that things are starting to pick up or maybe even—I don't know, maybe even that you made more profit than usual in the wake of this problem.

And I would be remiss if I didn't mention because people back home, and I don't mean just back home where I live, but back home where all of us live, cannot understand how the CEO of Equifax and the CEO of Yahoo! walked away with $90 million and $27 million and possibly a quarter of a billion dollars in stocks. This is unfathomable to the average person.

And I understand, Mr. Smith, you and I had an exchange in the Banking Committee where you said, "This was in the proxy, it's set by the board, it's not under my control." I understand all that. What I'm saying is regular people don't understand that, and they shouldn't understand how you harm consumers and then walk away with the amount of money that a small city or county uses for their annual operating budget. It's not fair and it's why this dais has an obligation to make a law and not just drag you back and forth and wave our fingers at you.

Thank you.

The CHAIRMAN. Thank you, Senator Schatz.

Senator Moran.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Thank you, Mr. Chairman. Thank you to the Ranking Member.

Let me start by asking this question. Let me set the premise, perhaps first to Mr. Smith and Mr. Barros, and then Ms. Mayer and Ms. Zacharia.

So a business makes a calculation, it determines probabilities, and it makes a decision about how it invests, in this case, invests in its data security based upon the probabilities of events happening.

And so my question is, before the breaches occurred with both companies, what did you expect? What did you say to your executive committee or to your board of directors, what's the probability of a breach occurring at our company? And then the second, the follow-up question to that is, what's that probability today?

So you calculated what the probabilities were, you make investment decisions about how to invest in security, and what that probability is. Is it any different today for additional breaches at either one of your companies than it was prior to the original breaches?

Mr. Smith?

Mr. SMITH. Thank you, Senator. I'd put in a framework like this, we don't calculate the actual percentage probability. We've got a very comprehensive framework called Enterprise Risk Management. I'm sure you've heard of that, ERM. And for 10 years or so we've always ranked data security as the most high-risk, high-probability risk we have as a company. If we had a security, cybersecurity event, it would be detrimental to the company. We don't calculate, is it 50 percent, 60 percent, 10 percent, or 5 percent, but we have——

Senator MORAN. Does that statement mean that you would expect a breach?

Mr. SMITH. The probability of a breach——

Senator MORAN. Is high.

Mr. SMITH. Yes.

Senator MORAN. OK. And is that calculation any different today, Mr. Barros, based upon the changes that you've made at the company? Is it still the same probability of a breach occurring today or tomorrow as it was prior to the earlier breaches?

Mr. BARROS. Well, we believe that today we are better than we were at the time of the breach for one reason. This was a pivotal

point in our industry and in our company, essentially. We have to make significant investments and continue to do so to make sure that we are better today and we will be better tomorrow.

Senator MORAN. So how much more money are you spending today to prevent a breach from happening than you were spending, as a company, prior to the earlier breach?

Mr. BARROS. As a natural response to the incident, we are spending significantly more money in that process.

Senator MORAN. But what percentage increase at your company has occurred as a result of what you learned from the breaches that have occurred in the past?

Mr. BARROS. We are expecting to have a specific spike on the costs for the——

Senator MORAN. Do you spend 50 percent more today than you did before?

Mr. BARROS. Easily.

Senator MORAN. Or 75, 100, 200 percent more?

Mr. BARROS. Four times more.

Senator MORAN. Four times more.

Mr. BARROS. Yes.

Senator MORAN. And as a result of spending four times more, would you say it's less likely today that a breach occurs at your company than the probability of it occurring before?

Mr. BARROS. This is my understanding.

Senator MORAN. And what's the reduction in probability?

Mr. BARROS. I don't have a specific number because we have a series of actions taking place today. I can say today that we believe that it is better today than it was before.

Senator MORAN. Would it be better if you were spending, instead of four times more, six times more? Is the technology out there that you could acquire to prevent this from happening——

Mr. BARROS. We are acquiring technology, and new tools, to make sure our security is strengthened and improved. We've been advised by specialists to make sure that we follow a sequence for installing this technology. There's a timing to do it.

Senator MORAN. Would Yahoo! answer this question in its circumstances?

Ms. MAYER. We have at Yahoo! one of the most valuable data bases in the world just because of the sheer number of users that are contained therein. We describe this as an arms race. Hackers become ever more sophisticated, and we have to become sophisticated in turn. So——

Senator MORAN. So would you have predicted a breach before it occurred? Would you expect a breach? I assume the answer to that's no, or you would have been doing something more?

Ms. MAYER. We did not calculate percentages and/or predict a breach. I will say we took significant efforts and investment to increase our security, which included increasing the size of the team by a factor of two. We did things like empowering our users to opt out of passwords and into something called Yahoo! Account Key. We increased our encryption, constantly changing the types of encryption we used to thwart hackers. We introduced a Bug Bounty where outside developers, if they discovered a vulnerability, could report it, and we would reward them. We hired outside teams

to attack us and tell us where our vulnerabilities were. We introduced machine learning to monitor our system and evolve with the hackers to ultimately identify when intrusions occurred. So we took extensive actions.

Senator MORAN. Let me turn to Ms. Zacharia. Is the probability of a breach less today at Yahoo! than it was prior to your acquisition of the company?

Ms. ZACHARIA. So, again, we don't calculate the probability of a breach, but what we do do is what our——

Senator MORAN. Well, let me ask the question differently then. Are customers more secure today than they were prior to the breach? Can a customer expect that it will have less expectation that their data is at risk than before the earlier breach?

Ms. ZACHARIA. Well, what I can tell you, Senator, is that Verizon has always taken security very seriously, and we're bringing that same focus and that same intensity that we've always brought to protecting our customers and our network to any new acquisition, including Yahoo!.

Senator MORAN. What seems to be missing to me, the assurance that, as a customer, however we define "customer," should have a sense that they're safer today than they were before, and I don't have any assurance from any of the response to my questions that that's the case, that we ought to be just as concerned today about a breach as prior to. And, you know, what I hear is that we're talking all these steps.

Let me ask you this question: Do you believe that other companies in a similar business, companies that have lots of data that would affect consumers if there was a breach, are they as vulnerable to breaches as your companies are and have been? This is not limited to Yahoo!, it's not limited to Equifax. Every other company that's in the data business is just as vulnerable as you have been and are still today?

Ms. MAYER. I would point out that the list of efforts that I discussed earlier were our ongoing defenses. In addition, in response to the breach, we took significant steps, causing our users to reset their passwords, changing our encryption, changing the attack surface area of our systems and the access that even internal employees had to those systems. So by all means, we did respond and change the level of protection given to our users.

Senator MORAN. And, therefore, today, as a customer of Yahoo!, I should feel how much better that my data is safe?

Ms. MAYER. I think it's difficult to quantify, but there is no question, in my mind, that the users are better protected today because these breaches were detected and remediated for.

Senator MORAN. Are you spending all the money necessary to increase that protection? Could they be safer if you did more, or are you doing everything you can do?

Ms. MAYER. I am no longer with the company——

Senator MORAN. That's true.

Ms. MAYER.—but I would say that certainly during my tenure, that was the case.

Senator MORAN. Ms. Zacharia?

Ms. ZACHARIA. Yes, and the security—exactly right, I agree—the security teams at Verizon would tell you that their job is to defend

against any and all attacker, and that's exactly what we're trying to do.

Senator MORAN. And the company provides them with the resources to accomplish that goal?

Ms. ZACHARIA. Absolutely.

Senator MORAN. Mr. Barros.

Mr. BARROS. It's the same for us.

Senator MORAN. And the final question is, Do any of you disagree that the Federal Trade Commission has jurisdiction over your data breaches and has the ability to regulate and to penalize for faults to prevent and then to penalize if there are breaches? Do you all agree that FTC is your regulator and has legal authority?

Mr. BARROS. Enforcing it.

Senator MORAN. Did you say unfortunately?

Mr. BARROS. I said that they make sure the regulatory perspective is in place.

Senator MORAN. OK. Thank you.

Ms. Zacharia?

Ms. ZACHARIA. Certainly for the Yahoo! incident, I'm not trying—so on the telecom side of Verizon, that's a little bit of a complicated question, but for the Yahoo! incident that we're here talking about today, absolutely.

Senator MORAN [presiding]. I understand. Thank you very much.

In the absence of the Chairman, I recognize Senator Baldwin.

STATEMENT OF HON. TAMMY BALDWIN,
U.S. SENATOR FROM WISCONSIN

Senator BALDWIN. Thank you.

I want to just start with a question of the panel: Mr. Barros, Mr. Smith, and Mr. Wilkinson in particular. Just identify if you have any information today about who hacked Equifax, who possesses the personal identifying information of about 145 million Americans, and what you believe they intend to do with it? Can you identify to me if any of you have that information today?

Mr. BARROS. No, we have no evidence.

Mr. SMITH. The only thing I'll add, Senator, is we engaged the FBI on August 2——

Senator BALDWIN. Yes.

Mr. SMITH.—and have been working with and cooperating with the FBI since August 2.

Mr. WILKINSON. In our experience, in the vast majority of these breaches, once the breach has occurred, everyone owns this data, because it's out in the public.

Senator BALDWIN. Thank you.

So we all know that the Equifax breach compromised the personal and financial information of more than 145 million Americans. And we really can't even begin to know what ramifications this failure will have to the families and individuals that are impacted. And I think it's clear that Equifax needs to do a lot more than it has to help victims respond to this breach.

Mr. Barros, will you make a commitment right here and now that Equifax will proactively notify every person who was impacted in this breach, yes or no?

Mr. BARROS. We have been notifying. We have been working with consumers. We have improved our webpage and are making sure that our social media efforts are active. We have been working with the consumers that have reached out to us, and I have a team working every day to make sure that we engage consumers.

Senator BALDWIN. I know that you have acted in areas where state law demands that you do so. Where it doesn't, are you going to reach out to each and every individual that you believe was impacted by this breach to let them know?

Mr. BARROS. We will execute according to the requirements that they have in the law.

Senator BALDWIN. And if there's an absence of law in a state, you won't do anything?

Mr. BARROS. We are actively engaging with consumers to make sure that they use the product that we have today.

Senator BALDWIN. Equifax set up a poorly functioning process where people would have to go to the Equifax website to find out if they were impacted. How many people have gone through this process?

Mr. BARROS. We have, as Mr. Smith mentioned in his statement the last time, we had close to—initially—for a period of time, we had close to 400 million hits.

Senator BALDWIN. Do you know how many individuals?

Mr. BARROS. 30 million individuals have——

Senator BALDWIN. 30 million?

Mr. BARROS. 30 million, yes.

Senator BALDWIN. Out of 145 million. You mentioned call centers in your testimony. Where are Equifax's call centers located?

Mr. BARROS. We have one call center in Lake City, Florida, and we have one call center in Nevada, in Las Vegas.

Senator BALDWIN. And where?

Mr. BARROS. The two major operations that we have are in Lake City in north Florida, where I visited a couple Saturdays ago, and one in Las Vegas as well.

Senator BALDWIN. Are there any out of the—outside of the United States?

Mr. BARROS. We use our—as a surge, for surge impact, we use call centers in Costa Rica—sorry. We use call centers in Costa Rica, we use call centers in other parts of the world. That's correct.

Senator BALDWIN. What other parts of the world?

Mr. BARROS. It varies from Malaysia, India. It depends on how the demand goes. Most of the calls that we have handled recently have been for specific problems have been here in U.S.

Senator BALDWIN. Most of them.

Mr. BARROS. Yes.

Senator BALDWIN. Equifax——

Mr. BARROS. Out of the surge. I'm sorry. Out of the surge. When we had a surge, we used the flexibility and capacity that we have.

Senator BALDWIN. Equifax is now offering free credit report locking for life, but only offering credit report monitoring through January 31, 2018. Will you make a commitment that Equifax will offer free credit report monitoring for life?

Mr. BARROS. We have the first service that was available, which is TrustedID Premier. That is actually valid for a year. So if you

enroll before the end of January, you have another 12 months to use the product with the five characteristics that have been described. The new product that we have put in place where consumers can lock and unlock their credit file will be available for free and for life at the end of January.

Senator BALDWIN. And monitoring?

Mr. BARROS. We don't have the scope of the project to offer monitoring at this stage.

Senator BALDWIN. Victims of this breach will really need to be able to control access to the reports from all three credit agencies to fully protect themselves. The other agencies charge between $5 and $10 for each and every freeze. Will you be offering rebates to the victims to cover their freezing costs with the other reporting agencies?

Mr. BARROS. Senator, I believe that the resolution has to be one that protects the consumer, it has to be sustainable, it has to be scalable, it has to be industry-driven, and we have to work with the government to make sure that we reach out to the consumers to execute that. We gave our first step forward, which was to offer a service that consumers can check and lock and unlock their credit data for free and for life. And we want to work with the industry to make sure that there is a similar capacity to do it for all credit reporting agencies.

Senator BALDWIN. Mr. Barros, your firm recently completed an internal review of the stock trades executed by four senior Equifax executives prior to the public disclosure of the breach and hack. The special committee report found that, quote, none of the four executives engaged in insider trading. The report failed to mention that Equifax's Chief Legal Officer, John J. Kelley, approved some of the stock sales on the same day that he called the FBI to alert it that the company had a problem. It took Mr. Kelley two more weeks to inform the executives that they were no longer allowed to sell stock. This is totally inappropriate, and yet the report does not even mention Mr. Kelley, and he still works for Equifax. I would like to ask both Mr. Barros and Mr. Smith, do you believe Mr. Kelley's failure to act was appropriate?

Mr. BARROS. I think it's not my perspective to provide if it was appropriate or not. The board has actively and conclusively determined that the four executives did the preclearance in a correct form. The board's special committee continues to investigate and review the process as it related to the cybersecurity incident, including policies and procedures.

Senator BALDWIN. Mr. Smith?

Mr. SMITH. The only thing I would add, Senator, is there was a full investigation by the independent directors of the board. You saw the report. It was published I think it was earlier this week or last week. The second thing I would say, it is not unusual for us to engage outside counsel, outside forensic experts, in this case, Mandiant, or the FBI. I mentioned earlier to one of the Senators, we have 3 to 4 million suspicious activities, suspicious attempts at our database around the world, so it's not unusual that—and, by the way, he didn't engage the FBI, it was the security team. That is not an unusual step in itself.

The CHAIRMAN [presiding]. Thank you, Senator Baldwin.

Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO, U.S. SENATOR FROM NEVADA

Senator CORTEZ MASTO. Thank you. And, first of all, let me just say thank you, Chair, and the Ranking Member for holding this hearing. I really appreciate that.

So let me start with Equifax and some of the concerns I have. I'm from Nevada, and there are about 3 million people there, and of the 3 million people, 1.3 million were impacted by this breach. In fact, I received over 4 dozens letters. Let me just give you an example of one of them. I have a woman in Carlin who wrote, "No citizen has a say in the reporting practices of businesses to credit bureaus. I did not choose Equifax to store my information, nor did my husband, nor any of our children, yet it is there, and clearly Equifax did not do enough to protect our information."

So a couple of questions to start with, and I want to drill down into the data that is collected because I think part of this is the data collection, and we should be looking at that. Equifax, my understanding of the breach of the 145 million consumers, the data that was collected was names of those consumers, Social Security numbers, addresses, birthdates, driver's license numbers, and credit card information. Is that true, yes or no?

Mr. BARROS. In some cases, yes; in some cases, no.

Senator CORTEZ MASTO. What other data do you collect on consumers besides the data that I just identified?

Mr. BARROS. Most of the data affected included Social Security numbers, name, date of birth, and address, that's it.

Senator CORTEZ MASTO. What other data do you collect other than what I just——

Mr. BARROS. We have a——

Senator CORTEZ MASTO. So I'm going to ask for the record, we'll submit that, if Equifax could provide me with that question, that would be very helpful, because I'm curious, does Yahoo! collect driver's license numbers?

Ms. MAYER. Not to my knowledge.

Senator CORTEZ MASTO. OK. So I think that's helpful in this discussion because to me the data breach that happened at Equifax is egregious. It happens all the time. We're all getting pinged. Government is getting pinged. Companies are getting pinged. We've heard it. I think, from what I've heard from Ms. Mayer, cybersecurity is a global challenge, we're always all getting pinged.

It is incumbent upon all of us, including the private sector, to not only have the top-line security, sophisticated security, always evolving with it, always ensuring that you're protecting that data, and when you fail to do that, then, yes, you should be held accountable, and the reinforcement should be swift, and consumers should be notified, and there should be restitution for those consumers. But we haven't had the discussion on the data. To me, that's what this is about because, quite frankly, even those individuals that you work with now and those consumers that had credit locks and credit freezes, their data was still breached, correct?

Mr. BARROS. Could be. If they——

Senator CORTEZ MASTO. Right. So it doesn't matter because that's what they're going to go after, is that Social Security number. And I see, Mr. Wilkinson, you're nodding yes. Isn't that correct?

Mr. WILKINSON. Yes, Senator.

Senator Cortez Masto: So shouldn't consumers be the ones to say, "I want to opt in or opt out when it comes to the data that I am sharing with you"? Don't you agree?

Mr. BARROS. Well, this is part of the way the economy works. When you—when the consumer goes and——

Senator CORTEZ MASTO. The consumer doesn't have a choice, sir. The consumer does not have a choice on the data that you're collecting. That's what I hear from my consumers. That's what I hear all the time. I know it. And quite frankly, the credit reports that I get as a consumer do not tell me all the data that you're collecting on me. Isn't that true?

Mr. BARROS. The credit report collects your—the trade lines that we have on your—for your——

Senator CORTEZ MASTO. That's true, isn't it? And let me just say I was attorney general for 8 years in the State of Nevada. Identity theft in the State of Nevada and across this country is through the roof, and every day we dealt with somebody whose identity was stolen. And what is so egregious about what you have done is now for the rest of their lives, the woman in Carlin and all of the people that I hear from Nevada, of the 1.3 million people whose identities were stolen, they are going to have to clear their record for the rest of their lives.

And what does that mean? That means that somebody is going to buy a boat in their name, a house in their name, people are going to commit crimes in their name, and, believe me, as a prosecutor, I've seen it. So they are spending the rest of their lives clearing their record and their good name, and that's why this is so egregious.

And I think you have an obligation not only to look at the data that you're collecting, but make sure you're protecting it, and if there is a breach, you are doing everything you can to remediate and bring restitution to those individuals whose information is stolen.

So let me talk to you because I've got a short period of time. Mr. Wilkinson, you talked about the data and Social Security numbers, and the idea that now we have to look at a different way of identifying the PII. I'm very curious if you have anything specific on what we should be doing when we're looking at that data and PII that is shared and collected?

Mr. WILKINSON. Well, the first thing to note, and it has been noted a few times, which is in the case of these breaches, in the case of this most recent breach, 145 million items of personal information was leaked. When you combine this with other breaches that have occurred, and there's a list of breaches that we could cite, we're getting very close to all of the personal information in the United States has already been breached in some way. So, of course, the question applies, which is, what are we trying to protect at this point?

In the case of some of the financial card breaches, like the Target breach from several years ago, or 3 years ago, that we actually testified, my company testified on behalf of the request to appear at that time, I think it was a good point to compare and contrast between what has happened with some of those breaches and in this case, and that is the financial payment system is reasonably resilient.

In that case, despite the fact that it was a burden for consumers, the ability for consumers to have a new card reissued, have that fraud remediated, and be back in business, the ability to do commerce, is relatively well known and relatively resilient. In addition, the liability largely fell to the financial institutions, the issuers of those financial cards, credit cards, and debit cards.

So I think looking to some examples like what we see in financial payments ecosystem is an example of a more resilient system than what we have in this form of identity today.

But our identities are out there, so I continue to reinforce that our position is that we would—we believe that a more resilient identity framework needs to be brought forward. There are several examples. I cited——

Senator CORTEZ MASTO. And I'm running out of time, and I know my time is up, but let me just say this. I agree with you, our identities are out there. Some of us are—it's too late.

Mr. WILKINSON. Yep.

Senator CORTEZ MASTO. But to our kids, it's not too late.

Mr. WILKINSON. Right.

Senator CORTEZ MASTO. And we've got to look to the future and protecting their information as well. So it is something that to me, we—it's not static. We've got to continue to figure out how we address this issue, if we're going talk about digital identities or the government coming up with something different. But I do agree with you, that there should be that public-private partnership. We've got to figure this out for the benefit of those people that we're taking their data, and they have no choice. They have no choice that companies are taking their personal information, they're monetizing it, and then they get stuck for the rest of their lives dealing with the results of a breach.

Mr. WILKINSON. Right.

Senator CORTEZ MASTO. So thank you.

The CHAIRMAN. Thank you, Senator Masto.

Senator Hassan.

STATEMENT OF HON. MAGGIE HASSAN,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Thank you, Mr. Chair.

And good morning to all of our panelists.

This is a question to the panel, although the most relevant example that we can call on is a response from Equifax this summer to the major data breach it endured. There are state-by-state laws requiring private and public entities to notify individuals when there are security breaches of their personally identifiable information. These laws represent the lowest amount of communication required. I'm interested in what companies are deciding to proactive-

ly do to help notify and help the consumers affected by these breaches.

So we could start perhaps with Mr. Smith and Mr. Barros. I know that you have both stated that Equifax has taken big steps to further the consumer satisfaction in their interactions with your company, but many of those steps seem to have come only after public outcry to your initial response.

So my question more broadly is, Can each of you elaborate on what considerations you and your companies take into account when determining steps to notify and remediate the damage done to consumers from data breaches?

Mr. SMITH. Senator, if I may start, and, Mr. Barros, if you want to add on, one of the notification processes we took obviously very seriously, the state requirements as far as time and notification——

Senator HASSAN. But, of course, I'm asking beyond that because those are minimal. So what are you guys now deciding to do beyond that? And how do you—what considerations are you making?

Mr. BARROS. Well, my top priorities have been our consumer response and hardening our security system. This is what I mentioned at the beginning. On the consumer side, we definitely made our call centers more scalable. We improved our platforms. So in other words, you can get in and out—you can have access within 3 minutes, you can have a response back from Equifax. It is——

Senator HASSAN. But I am also talking about your proactive efforts to notify consumers beyond the requirements that state law, for instance, gives you.

Mr. BARROS.—correct. Now, with the amount of hits that we have, we've been working with the consumers to make sure that they use the services that we have provided for free for them for the transition period, and we will continue to do that. We are going to introduce our new app, which will allow consumers to lock and unlock their Equifax credit file, for free, for life.

Senator HASSAN. Well, Mr. Smith.

Mr. SMITH. Senator, the one thing I'd add is that the process we did use was, one, legal and acceptable, and it seemed like it worked. He mentioned we had four——

Senator HASSAN. Again, I——

Mr. SMITH.—consumers.

Senator HASSAN.—we can pursue this on the record. That isn't my question, and I want to get to the other panelists. I'm asking for now, regardless of—state laws, at a minimum, you have to follow it. But what are the factors that you are considering when you decide when to notify a consumer? And if any of the other panelists would like to answer just very briefly, that would be helpful.

Ms. MAYER. At Yahoo!, we generally took a proactive stance due to the global nature of our business, which is to say, yes, laws vary from state to state, but our view was frequently if user notification was required anywhere, we did it everywhere——

Senator HASSAN. Right.

Ms. MAYER.—and we endeavored to be both accurate and comprehensive because accuracy and comprehensiveness are very important, as well as analyze how any data might have been misused or abused, and also be swift in the response.

Senator HASSAN. Yes, ma'am.

Ms. ZACHARIA. Yes. At Verizon, what we do is first we always obviously look at what the law requires, but then we look at what we think is the right thing to do for the customer. And if in a particular situation we think it's the right thing to notify the customer, then that's what we do.

Senator HASSAN. Thank you.

Mr. WILKINSON. Our company doesn't hold consumer information, so it's not applicable.

Senator HASSAN. I didn't think so, but just checking.

I wanted to follow up with Mr. Barros about the difference between credit lock and credit freeze services. Placing a freeze on their credit is one of the best ways consumers can protect themselves, of course, from identity fraud. Equifax has stated that it will waive the fee for consumers to place a freeze on their credit for several more months in response to the major data breach earlier this year.

At that point, the company has stated, and I believe you stated in your testimony, Mr. Smith, that it will offer consumers the ability to lock their credit for free. Can you please share with the Committee the legal differences between a credit lock and a credit freeze in terms of consumers' rights and protections, and who has access to a consumer's credit report when it is frozen versus locked?

Mr. BARROS. Fundamentally, there is no difference between a lock and a freeze. When you freeze—when you freeze, you use a regulatory process to do it, and you make a phone call, you identify yourself, you get a PIN, and you're ready to execute a freeze or not. The reason why we're offering a lock product is the simplicity of the process. So in financial institutions, they are trying to get to your file to open an account, and won't be able to do that in either situation, if the file is frozen, or if the file is locked.

Senator HASSAN. Well—and I see that my time is up—I think there are experts who would disagree with you in terms of your statement that there is no difference between a freeze or a lock. And one of the things I will follow up with you in writing about is the degree of fees that Equifax gets from helping consumers unfreezing or unlocking their information.

I thank you for your indulgence, Mr. Chair.

The CHAIRMAN. Thank you, Senator Hassan.

Senator Capito.

STATEMENT OF HON. SHELLEY MOORE CAPITO, U.S. SENATOR FROM WEST VIRGINIA

Senator CAPITO. Thank you, Mr. Chairman.

I think all of the panelists for being here today.

I want to start with a simple question to Mr. Barros. To your knowledge, has any of the information that was breached—driver's license, Social Security, birthdates, addresses, credit card information—do you have any indication that any of those customers that you—or folks whose data was breached has been misused, or did you have any indication that somebody was using this data to make other purchases or other things of that nature?

Mr. BARROS. To the best of my knowledge, it's premature to make an assessment that it has been used already.

Senator CAPITO. Mm-hmm, mm-hmm.

Ms. Mayer, what about in terms of Yahoo! and the data that was breached there? Did you have any indications at Yahoo! that an individual's data had been misused? Was that a red flag that was brought to your company?

Ms. MAYER. No, we saw no volume of reports. We did roll out a program advanced protection against threats that notified users if we saw any indication that their account might be accessed by a state-sponsored attacker, and we rolled out that program I believe in 2015. So users are notified in real time if there is any suspicious activity on their accounts.

Senator CAPITO. Right.

So, Mr. Wilkinson, in light of the fact that you said all this information is in the public domain, not just with the bad actors, but out there in general probably, we would have to assume that, I mean, you're assuming that, I would assume that, does it surprise you that none of this information that's out there has been used in a nefarious way that anybody can detect at this point?

Mr. WILKINSON. Yes, it would surprise me if none of it had been used in a nefarious way to this point given the timeframe that we're talking about.

Senator CAPITO. Yes, and that surprises me as well.

Mr. Barros, you mentioned in terms of how individuals were contacted, that obviously Yahoo! has a direct communication with their customers through their e-mail accounts. All of the data that's collected here does not seem to indicate any kind of e-mail address or phone number that you can send out a mass warning signal. So your customers basically have to opt-in to find out. And you said you've been out on social media telling the ways to do that.

Will that change your profile in terms of being able to have quicker, more efficient, and wider spread way to disseminate information to those of the folks who have information that you're collecting, some kind of a communication tool with all these individuals?

Mr. BARROS. It frustrates us as well, because we would like to have more proactive engagement with the consumer. As I said, we have improved significantly our website. It's much more user friendly today. It's easier to access. We have more phone numbers available for consumers to ask questions. These phone numbers are public. Our website has these phone numbers as well.

We are proactively doing this through social media, inviting people to talk to us——

Senator CAPITO. Right.

Mr. BARROS.—to make sure that we can respond and direct them to the right solution.

Senator CAPITO. Well, I can tell you that one of the ways that people want to talk to you is when they get their credit report and see something on there that they don't agree with, and I think that your company through the years, and the credit bureaus in general, have realized that this is an enormous problem for the American consumer if there's a false entry on their credit report, especially if it's one that knocks down their credit rating. And I'm sure—I

know that happens frequently, and I know you've worked to try to correct this problem and try to reach the consumer.

But I would hope that, having tried to do this myself with my own personal credit report and experiencing how frustrating it is to get through to whoever I was trying to get through to, Equifax or the other two credit reporting agencies, to try to register a complaint and work through the process, it's very time-consuming and difficult.

So I'm going to assume that those processes are tightening up, particularly in light of this security breach that we've seen at your company in terms of consumer-friendliness.

Mr. BARROS. Right. One of the top concerns that I have is how to improve our response to consumers. We are looking at this process to make sure that we have a better way to communicate with consumers.

Senator CAPITO. And I'm also interested in your proposal to lock your information as an individual that you said you would have on-stream in January at cost-free where the customer could opt-in and then opt-out, unlock and lock their own personal data. How does that work in terms of your business framework? If a consumer locks the data out, are you then locked out to reporting to your customer how that customer's data would influence their credit rating in terms of purchasing a home or something like that?

Mr. BARROS. Yes, it's part of the process. So the objective that we have when we designed this service was to make sure that the consumer would have the power in their hand to lock and unlock their file——

Senator CAPITO. So when they have a locked file, it's locked from you disseminating it to anybody?

Mr. BARROS. Yes, nobody can have access to that information in their file.

Senator CAPITO. OK. Thank you.

The CHAIRMAN. Thank you, Senator Capito.

Next up is Senator Gardner.

STATEMENT OF HON. CORY GARDNER,
U.S. SENATOR FROM COLORADO

Senator GARDNER. Thank you, Mr. Chairman. Thank you to our witnesses for being here today. I hear a lot of conversations about your file, meaning your personal information. I've heard it said that this is consumer information, this is personal identification information.

Mr. Barros, can you tell me who owns the information that you provide to your clients, customers?

Mr. BARROS. According to the existing regulatory framework, we own the information.

Senator GARDNER. Does the consumer have any ability to say, "I don't want you to have that information"?

Mr. BARROS. They have the opportunity today to lock and unlock their file, and, therefore, not allow anyone to have access to it.

Senator GARDNER. But do I have an ability to say, "I don't want Equifax to have any information about me"?

Mr. BARROS. I understand that from the regulatory framework that we have today, the consumer cannot delete their file.

Senator GARDNER. So the answer is no. So I, as a consumer, apply for a credit card or a bank loan. That institution then provides it to you, and I have no ability to stop that from happening.

Mr. BARROS. You can lock and unlock your file.

Senator GARDNER. So the answer is no, I can't stop that. And the answer is no, I can't prevent you from getting it. So whose information is this? Is it my file or is it your file? Whose file is it?

Mr. BARROS. According to the regulatory perspective, I have the information——

Senator GARDNER. So it's your file, not my file. So all the information about me, all the consumer information I produce, all the data, everything that I own that defines my life, I have no control over that. Is that correct? Other than you've got it and I can tell you whether I want you to give it or sell it to somebody else.

Mr. BARROS. This is how the industry framework——

Senator GARDNER. I get it. I get it. Do you think it's right, though?

Mr. BARROS. I think it's not my perspective to say it's right or wrong. This is the regulatory perspective that we work under.

Senator GARDNER. Who owns the credit card information that you have on me? That's you then at that point, correct?

Mr. BARROS. I just have a trade line on the credit card information.

Senator GARDNER. So do you think consumers should own their data?

Mr. BARROS. I think my——

Senator GARDNER. Ms. Mayer, should consumers own their data, own their own information?

Ms. MAYER. Yes, I believe that they should.

Senator GARDNER. Should we be able to control our own information, Mr. Barros?

Mr. BARROS. Yes. This is the effort that we're making through the process, where consumers should control the information that we have, the credit——

Senator GARDNER. But you're saying by putting a lock or an unlock that can be hacked by somebody is consumer control?

Mr. BARROS. If you lock and unlock—when you lock and unlock your file, nobody can have access to your file.

Senator GARDNER. Would you support a mechanism that allowed consumers to say, "I don't want that information to go to Equifax, Experian, TransUnion"?

Mr. BARROS. This is a decision that is bigger than our industry. I think we need to understand how the economy is going to behave in that situation.

Senator GARDNER. Mr. Smith, it's my understanding that the data access through Equifax's consumer dispute portal was not encrypted at rest. Is that correct?

Mr. SMITH. Correct.

Senator GARDNER. If the answer is yes, as you said it was, was the fact that this data remained unencrypted at rest the result of an oversight or was that a decision that was made to manage that data unencrypted at rest?

Mr. SMITH. There are multiple tools we use and used to use when I was there to secure data: encryption at rest, encryption in

motion, tokenization, masking, firewalls, multiple layers of security. Encryption is only one. If you look across our——

Senator GARDNER. So a decision was made to leave it unencrypted at rest?

Mr. SMITH. Correct.

Senator GARDNER. Mr. Barros, since you took over, as part of your internal response to the breach, have you directed the company to encrypt such data, or have you been recommended to encrypt such data, so it is encrypted at rest?

Mr. BARROS. We have done a top-down review, a comprehensive top-down review, of our security situation. We use outside companies to help do that: PwC and Mandiant. We are strengthening——

Senator GARDNER. So let me just—a yes-or-no question, Does the data remain unencrypted at rest?

Mr. BARROS. It's going to be part of the process that has been reviewed——

Senator GARDNER. Yes or no, does the data remain unencrypted at rest?

Mr. BARROS. I don't know at this stage.

Senator GARDNER. You don't know if this—this is the reason why it was breached, is that correct?

Mr. BARROS. This——

Senator GARDNER. This data was unencrypted.

Mr. BARROS. Encryption is one form of defense. We have several forms of defense and tools in place now that can help prevent this from happening again.

Senator GARDNER. And the data remains unencrypted at rest.

Mr. BARROS. We have deployed several different tools, and encryption is one tool.

Mr. SMITH. Senator, if I may. It's my understanding that the entire environment in which this criminal attack occurred is now much different. It's a more modern environment with multiple layers of security that did not exist before. Encryption is only one of those levels of security.

Senator GARDNER. There are other experts, the privacy experts here. Is it a reliable, safe methodology to leave this data unencrypted at rest?

Mr. Wilkinson.

Mr. WILKINSON. I think we've spoken of the high value of identity information and what it can be used for today. Certainly, as Mr. Smith noted, encryption is one of the tools, but certainly from our company's perspective, a very important one to be used for data that is data of this type that is of high value.

Senator GARDNER. So your answer is——

Mr. WILKINSON. Yes.

Senator GARDNER.—it is irresponsible to leave this unencrypted at rest.

Mr. WILKINSON. Other segments of the industry, I've mentioned a few examples, of the payments ecosystem have PCI requirements that require this kind of information, credit card data at retailers and things like that, to be encrypted. In this case, it was not.

Senator GARDNER. When, Mr. Smith—I know my time is expired, if I could ask one more question—when specifically did you notify the other credit reporting agencies about the breach?

Mr. SMITH. Senator, we notified them when we notified the public.

Senator GARDNER. So the public and the other—and that was around August. Can you give me the date again?

Mr. SMITH. September 7 was when we went live with the——

Senator GARDNER. September 7. The breach occurred August 2. September 7?

Mr. SMITH. No. We saw suspicious activity on the twenty-ninth and thirtieth of July, notified the FBI the second——

Senator GARDNER. The second. I'm sorry, that was the second, yes.

Mr. SMITH. That's when we notified the FBI. And we went public with it on the seventh of September.

Senator GARDNER. So the seventh of September is when the other credit rating agencies also received that information.

Mr. SMITH. That's when we went public with the entire breach, yes.

Senator GARDNER. Thank you. Is Equifax currently under investigation by the Department of Justice or SEC?

Mr. SMITH. There are multiple investigations.

Senator GARDNER. Thank you.

The CHAIRMAN. Thank you, Senator Gardner.

Senator Young.

STATEMENT OF HON. TODD YOUNG,
U.S. SENATOR FROM INDIANA

Senator YOUNG. Thank you, Chairman.

I thank our panelists for being here today.

Ms. Mayer, you were CEO of Yahoo! at the time of the largest data breach in all of human history, the so-called 2013 and 2014 breaches. You've testified here today that the 2014 breach was state-sponsored, but you have not concluded that the 2013 breach was state-sponsored, is that correct?

Ms. MAYER. We have not been able to determine who perpetrated the 2013 breach.

Senator YOUNG. OK. Thank you. You've testified today you didn't learn of either data breach until 2016, is that correct?

Ms. MAYER. I learned of the breaches at the scale reported in 2016 in December——

Senator YOUNG. What does that mean?

Ms. MAYER. In December 2014, we saw a Russian intrusion in our network, and we saw 26 individuals all with Russian connections and political interest in Russia with accounts compromised. We notified the FBI, and we put in place a special notice for those users that had to be dismissed by user action to make sure they were aware that this had happened.

Senator YOUNG. Thank you. Is it correct that you didn't learn of the 2013 breach until 2016?

Ms. MAYER. That's right.

Senator YOUNG. OK. What sort of information can you provide this Committee that supports your claims, that you didn't learn of the 2013 breach until 2016?

Ms. MAYER. Our board formed an independent committee, and they have reported on their findings.

Senator YOUNG. OK. And that's all publicly available?

Ms. MAYER. Yes.

Senator YOUNG. OK. Thank you.

Mr. Smith, Mr. Barros, the former and current CEOs of Equifax, I'm grateful for your presence here today. I represent over 6.5 million Hoosiers. 3.8 million Hoosiers, 3.8 million Hoosiers, 60 percent of Indiana's population, was impacted by Equifax's data breach. Can you see why they feel like companies like Equifax don't have their back? Yes?

Mr. SMITH. Yes, Senator.

Senator YOUNG. OK. You know, one of the tragic things about this whole episode is that many of these Hoosiers, many Americans won't discover until a number of years down the road that there was in fact a data breach. A single mother of a few children gets a new job in Gary, Indiana, goes to buy a car because this job requires her to drive, and she finds out her credit has been ruined. What is Equifax going to do to remedy the situation for that single mother?

Mr. SMITH. Let me jump in first, maybe then you can add to it.

That was the idea behind the lifetime ability to lock and unlock your file we talked about in four prior hearings. If it's locked, Senator, you don't have the ability to go rent a house falsely in your name or rent an apartment, get access to a credit card.

Senator YOUNG. That's prospective and prophylactic, defensive, and it seems like a good thing to do. Let me return to that momentarily.

I will say, you know, we've had these massive data breaches, and it is effrontery to the basic sense of fairness to most Americans that the top executives leave with tens of millions of dollars. I'm not trying to make a class warfare argument, but when I see the United States Navy just fired two top officers in the Pacific on account of some sailors that died in the wake of the USS John McCain situation, and they were separated from the military service because of a loss of confidence, I think this is an issue that we collectively in Congress need to start discussing more seriously.

If the titans of free enterprise here in the United States of America don't take more seriously—and I'm talking about boards as well as executives—when things like this happen, it's just—it offends the sensibilities of most Americans. Can you understand that, why that would offend the sensibilities of Americans, for them to be on the receiving end of a data breach, and within months, somebody leaves with tens of millions, maybe hundreds of millions, of dollars?

Mr. SMITH. I understand your point, Senator, but as I've said in prior testimonies, I left with nothing except a pension. I've asked for nothing. I waived my bonus. There is no equity coming next year. I'm working for 3 months to 6 months, as long as needed for free, in an advisory capacity.

Senator YOUNG. Yes.

Mr. SMITH. What I'm walking away with, it was all disclosed in the proxy, is my pension.

Senator YOUNG. Yes.

Ms. Mayer, you don't need to answer the question. I don't mean to personalize it, I'm just talking about culturally, big business in this country.

I would like to touch on one policy issue before I move forward. So the idea of the credit reporting agencies moving forward will give consumers the right to request a locking of access to their credit files at no cost to them.

Can you pledge, Mr. Barros, that 5 years from now, Equifax won't be charging consumers to lock and unlock their credit files? And would you be opposed to Congress implementing a law today that states unequivocally that industry can't charge to lock or unlock an unlimited number of times each year?

Mr. BARROS. Thanks, Senator. The proposal that we have put forward, which we definitely expect to lead the industry in that direction, where consumers can lock and unlock their files, is free, for life. This is a commitment that I have made, and I definitely welcome the conversation with the rest of the industry and the government.

Senator YOUNG. Thank you for that. Thank you all.

The CHAIRMAN. Thank you, Senator Young.

Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman, and thank you for holding this hearing. We've had several larger Commerce Committee hearings on cybersecurity, certainly had some in the Energy Committee, and I think Homeland Security has had some. I think the Armed Services Committee has had some.

I think now is the time for us to be very serious about passing legislation, as we did out of the Senate, that would help us fight the issue of cyber crime, and particularly help strengthen our critical infrastructure against state actor attacks, as Ms. Mayer mentioned. But these aren't the only things that are being attacked; our networks at nuclear power plants, our pipelines, a whole variety of things.

And as we continue to grow the economy of the Internet of Things, in the hearing we just had, I guess that was yesterday, we also heard about how more devices and more connectivity means more data entry portals for people to attack. So a couple of things about—so I hope our Committee will join in the efforts to get cybersecurity legislation over the goal line this year. I think it's not too soon to act.

I, too, want to bring up that there are 3 million Washingtonians that were impacted by the Equifax, according to my information. It's my understanding, Mr. Barros, that a patch was available that was not implemented, like a basic hygiene issue wasn't followed. Is that correct?

Mr. SMITH. That is correct.

Senator CANTWELL. Why can't Mr. Barros answer that question? Because he doesn't know or because——

Mr. SMITH. He was not in the position at the time.

Senator CANTWELL. OK.

Mr. BARROS. Yes, I came to the position 6 weeks ago, and my understanding is the same as Mr. Smith's, that what happened was a combination of human error and technology. I defer to him because he actually lived through this process.

Senator CANTWELL. What was the technology error if a patch was available and it wasn't implemented by an employee? And the reason I'm asking you about this——

Mr. BARROS. Sure.

Senator CANTWELL.—and I understand the dual role here, but my point is this: we have to do both. The issue of cybersecurity is here, it's here. It's a national security issue, it's a consumer issue, it's a, you know, future issue on identity theft and the ability for individuals to protect the things that they hold dear.

So we have to do both. We have to, at the Federal level, up our game and make sure that we're making investments to help on critical infrastructure and certainly addressing this issue on an international basis. What do we need to put into place on an international basis to get people on the same page in fighting cyber crime? We have to do that. But at the same time, we need to make sure that everybody gets hygiene and that the hygiene of your day-to-day business and even your home computer and everything else is going to be a critical aspect of the world that we now live in. So I want you to know and be able to speak to the fact that, you know, one individual failing to put a patch in place caused this much damage.

Mr. BARROS. Since I got to this job, my first priority has been to harden our security systems. We have done a comprehensive review of the process: improving our patching capabilities, improving our tools, updating our tools, and making sure the vulnerability detection process is much more up to speed at this stage. We have changed our policies to make sure that we have redundancies and "closed loops" in place to improve the accuracy and precision of our execution.

Senator CANTWELL. Do you think it's good enough to have voluntary safeguards for the industry, or is it time to have something more stringent?

Mr. BARROS. I understand the safeguards that we have. I think they provide the scope in which we complied with the scope before. The industry is ahead of that in many perspectives, deploying new tools, using new tools. We definitely welcome the conversation.

Senator CANTWELL. I would say that we need something more at this point in time, that if on the hygiene issue, one employee was able to miss something as critical as this and put so much data at risk, that we need something to make sure that this is implemented.

Does anybody else on the panel want to answer that question?

Mr. Wilkinson?

Mr. WILKINSON. The vulnerability that we're speaking about, now that you want the specifics of it, was called the Apache Struts. It came out—we were aware of it in March, we became aware of it in March publicly. This is a zero-day vulnerability. These types of vulnerabilities are serious, and they happen more often than we'd like to speak about. When we become aware of zero-day threats, our need to react to those kinds of threats is quick and has to be conclusive.

This is something that we're going to continue to see. It's not new, it's going to continue to happen. This concept that you continue to speak about, Senator, of cybersecurity hygiene is a very

important one, because I liken it a little bit to locks on doors. We can speak for a bit about the fact that no matter what we do, there is still some vulnerability in our ecosystem, there is some possibility that we'll be breached, but some of these best practices are, frankly, just like locks on your front door. Just because that's not going to protect you against all crime, you still put a lock on your front door. Good cyber hygiene includes things like reacting quickly to zero-day threats.

Senator CANTWELL. Exactly. That is my point exactly. Thank you so much for that because you just explained that you have to have—we have our national labs working day and night against the unbelievable amount of attacks that are happening every single day. We have all of this effort that we're now going to try to do both in getting a skilled workforce that this Committee had a hearing on to doing everything, but we need companies to follow a hygiene with great religious feverance. I believe that we have to help do our part, too, because if state-owned actors are going to continue to hack, we need to do something, but we need the companies to follow a hygiene and be very religious about it.

Thank you, Mr. Chairman. I know my time has expired.

The CHAIRMAN. Thank you, Senator Cantwell.

Next up is Senator Peters.

STATEMENT OF HON. GARY PETERS,
U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Mr. Chairman, and thank you so much for putting together this hearing. This is an incredibly important topic, and I think it angers most folks as they hear about this incident and the impact that it's going to have on over 140 million Americans in the case of the Equifax breach, over 4 million in my state. And I just want to pick up and expand a little bit before I have some questions on Senator Cantwell's questions to Mr. Wilkinson.

My understanding—I just want to be clear of this—this was a vulnerability that was discovered, there was a patch created. The information went out. And that means, what my understanding is when these go out, bad guys find out about them as well. You're basically broadcasting that there is a vulnerability that people can figure out pretty easily. So at least some of the experts I've talked to have said this was not a sophisticated hack, it was a pretty simple hack because the roadmap was pretty much put out for folks to take.

So we've had discussions about national or state actors involved, highly sophisticated networks. This was just basically a roadmap was put out for the bad guys, and they jumped in and got in. Is that correct?

Mr. WILKINSON. It is. I think that it goes back to the discussion of when zero-day threats are publicized, they do create a bit of a roadmap for the bad guys, as you said, which is one of the reasons why the need to respond quickly to close down those types of threats in your ecosystem is very, very important.

Senator PETERS. Right.

Mr. WILKINSON. Again, it's best practices, it's hygiene.

Senator PETERS. Well, and I just want to paint the picture for the American public to know that basically a roadmap was put out for all the bad guys out there who want to do us harm, that there is a vulnerability, and we have a company that has some of the most sensitive personal information about each and every one of us, and as we heard from testimony earlier, we don't have any choice in the matter. Companies can collect all this information, and they don't even take the time to look at a roadmap that has just been out that there's a breach.

You know, I can't think of a clearer definition of gross negligence anywhere. A company that has been entrusted with this most sensitive data, and customers didn't have a choice for you to hold it, and you're holding it. I didn't ask Equifax to have that information. No one asked to do that. You're holding that, and you don't take the precautions when a roadmap has been put out.

So I guess, you know, the other question to you, Mr. Wilkinson, is that after a breach has occurred, is it oftentimes a criminal may wait some time, too, before using this data?

Mr. WILKINSON. Absolutely.

Senator PETERS. So this may be a while before we actually see it being used?

Mr. WILKINSON. Yes.

Senator PETERS. Can you say, in your professional opinion, is there ever a point after a breach, especially one of this magnitude, where consumers can no longer fear the formation of fraudulent accounts where this could be used against them?

Mr. WILKINSON. No, Senator. I think that goes back to my original comments, which is this type of data being out in the wild, if you will, is forever now exposed and will never be credibly used for secure identity again.

Senator PETERS. So we have to worry about this the rest of our lives.

Mr. WILKINSON. Yes.

Senator PETERS. So we have to worry about this the rest of our lives.

Mr. Barros, you mentioned that there is free credit monitoring for one year. Is that correct for folks who may have been victims of this?

Mr. BARROS. Yes. It started since we announced the breach on September 7. We extended the opportunity to enroll until the end of January, and after that point, you still have 12 months of free credit monitoring.

Senator PETERS. So why only 12 months when we've heard that we have to worry about this the rest of our life?

Mr. BARROS. Because we believe—I believe, I strongly believe, that the actions that have to come out of this incident have to be to protect the consumers.

Senator PETERS. For one year.

Mr. BARROS. No, for——

Senator PETERS. Why not for the rest of their life, which is the——

Mr. BARROS. The product that we have offered today is a step forward in that direction where the consumer can lock and unlock their file, and it's free for life.

Senator PETERS. But that is only with your company. This information, as we heard, can now be used for any of the other access to any other credit reporting agencies. There are all sorts of avenues now that you can basically use this information to create a false identity, and you're saying that your response, as a company, you can lock your credit with us going forward, but you still have vulnerabilities with all of the other agencies. They'll just go to—I mean, this is pretty simple if you're a bad guy, just don't go to Equifax, go to one of the others. I've got the keys to the kingdom. I'm going to go other places.

You know, we have to create incentives, and I've heard that from the panelists, incentives to stop this type of behavior and to make sure people put the highest standards in place, and certainly gross negligence should never be acceptable. To me, what we need to do is, from an incentives standpoint, is if you're giving information of mine, and I did not ask to have that information given, I understand you make money when you provide information to financial institutions, you make money on my information, which I have never asked you to use.

At a minimum, you should let me know you're making money off of that information, and I should actually give you permission to give my information out. If you're going to make money, I don't understand why I don't have the ability and the tools for any kind of agency right now to be able to make sure that I have control, as we've talked about. This should be my information that we control.

So I'm out of time right now, but I think, you know, this raises a host of major issues related to privacy and control of data. And right now, we don't have the kinds of incentives to get companies to really protect that information. You profit from that information. You don't protect that information. You allowed a simple, unsophisticated hack to have access to 140 million people's most private information.

There needs to be some strong liability. Companies that do not protect information and jeopardize Americans for the rest of their life need to be subjected to strict liability and need to be stepping up and making sure that those consumers are protected for the rest of their lives. And hopefully that's something we can consider as we move forward in this Committee.

Thank you so much.

The CHAIRMAN. Thank you, Senator Peters.

I have Senator Markey has returned. Senator Markey, Senator Duckworth, and Senator Klobuchar.

STATEMENT OF HON. EDWARD MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman, very much. Mr. Chairman, the public wants us to do more to protect their privacy and security, yet earlier this year, Congress formally rescinded the Federal Communications Commission's broadband privacy and security rules, which ensured that broadband companies, like Verizon, adopt reasonable data security protections.

These protections ensured broadband providers implement up-to-date best data security practices, provide appropriate oversight of

security practices, properly dispose of sensitive information, and notify affected consumers within 30 days of a breach. Yet, Verizon opposed these data security and privacy protections and played an instrumental role in ensuring that they were, in fact, repealed.

Broadband providers, like Verizon, argued that we needed a light-touch regulatory framework like those governing websites like Equifax and Yahoo!. Well, 3 billion Yahoo! account users and 145 million Americans have now learned that light-touch means hands-off, light-touch means no protections, light-touch means free rein. And now, because of congressional action, free rein for broadband providers, like Verizon, to collect, use, share, and sell consumers' most sensitive information without their consent is the law, free rein to ignore reasonable data security protections and avoid promptly notifying consumers when their sensitive information has been compromised.

Ms. Zacharia, your testimony states that security has always been in Verizon's DNA. And during today's hearing you stated that Verizon would support national data security legislation. But Verizon actively and vigorously lobbied to eliminate these data security and privacy breach notification protections. How are these two positions consistent?

Ms. ZACHARIA. Senator, Verizon believes that there should be a single national framework when it comes to data security and privacy. We do support legislation in both of those areas, and we'd be very happy, as I said earlier, to work with your office or other members of this Committee on what that legislation should look like, but we do think that there should be one overarching framework, and the CRA was not that.

Senator MARKEY. Yes. Well, here's where we are: now we have nothing. You know, now we have nothing. So you repealed the law that actually required that there be protections. Now we have nothing.

And from my perspective, you didn't have to repeal one of the most comprehensive data security and privacy frameworks to develop a national data security framework. You could have advocated for Congress to give the Federal Trade Commission the authority to prescribe data security protections to websites as well. Instead, Verizon opted to eliminate the rules altogether.

So that's the problem that we have right now, that we had very strong, you know, data security and privacy protections that were on the books, and they were removed as part of a CRA, a vote on the floor of the Senate and the House earlier this year.

So as we sit here, we hear concerns about the need to have legislation. We had it. We had it. And it was going to actually work in terms of ensuring that we would have those regulations that would be put on the books. But, instead, we don't have anything.

So I guess in retrospect, do you think it was in the public interest to eliminate these data security and breach notification protections, Ms. Zacharia? If you could go back in time earlier this year, would you still remove those protections from the books?

Ms. ZACHARIA. Yes, I would, Senator. And, again, we do think that there should be national data breach——

Senator MARKEY. Right. No, I appreciate that. We had it. You advocated strongly to remove the protections. OK? That's what you

did. And even today you're not regretful at all. OK? But that's going to be the environment within which we're working right now. That's where Yahoo! was. That's where these other companies were over in FTC land. OK? And we had a stronger regime that was in place and going to be made even stronger.

And that's, in fact, what the American people want. They want real teeth to be put into these laws. They want real accountability from the private sector in terms of the guarantee that there is real security around this data that goes right to the very identity of who people are as citizens of our country. And instead of toughening those laws this year, there was a weakening, a serious weakening.

And I think ultimately we're going to pay a big price as year after year goes by because ultimately it's not talk, it's going to be action that makes the difference. And those actions had been taken, they were on the books. They were starting to put a little teeth into the protections, and now that is gone.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey. Obviously some of us have a difference of opinion on that subject. I think there are ways that we can address data breach that don't specifically have as their principal objective enriching class-action lawyers, but I do think rather than rehashing that debate, we ought to be looking at what we can do to prevent breaches. I'm sure that government enforcement agencies, like the FTC, which can help make consumers whole, have the tools they need to hold bad actors accountable.

Next up is Senator Duckworth.

STATEMENT OF HON. TAMMY DUCKWORTH,
U.S. SENATOR FROM ILLINOIS

Senator DUCKWORTH. Thank you, Mr. Chairman, and also thanking the ranking member for convening this important meeting. As today's proceedings made clear, the harm caused by these massive data breaches is incredibly far-reaching. And I just want to take a moment to highlight how both states and Federal Government entities rely on these agencies, such as Equifax, for services, for credit monitoring—for credit services.

For example, Equifax's loss of millions of Social Security numbers endangers the well-being of our nation's veterans, who receive VA disability benefits. Now, at the current time, the VA allows veterans to use a wide variety of methods to interact with the Department. If a veteran is not comfortable going online, he or she can actually manage their disability benefit account by fax.

So, for example, a veteran can fax a request to change the bank account into which their VA disability benefits are deposited, and those changes will be made if the form includes a Social Security number that matches the name of the requestor. This policy and process was likely created in an era when your valid Social Security number could serve as an effective authentication tool. Obviously, that is no longer the case.

So my initial questions to you, Mr. Barros and Mr. Smith, is simple. Following Equifax's loss of millions of Social Security numbers, what concrete steps did the company take to notify government agencies, and specifically the United States Department of Vet-

erans Affairs, of the urgent need to strengthen authentication policies to prevent service-disabled veterans from having their benefits stolen?

Mr. BARROS. We have—my team has actively worked with the Department of Defense, the veterans associations, the Department of Veterans Affairs, the CFPB, and the Senate, in order to make sure that we enhance the communication process and have solutions that allow military service members to be informed about how to protect themselves using our services.

Senator DUCKWORTH. So when you went public with the information on the breach, when did you contact the DoD or the Department of Veterans Affairs to inform them of the significance of the breach and what they would have to do to strengthen their processes?

Mr. BARROS. I can say what I did since I got here. I asked my people to make sure that they contacted DoD and the veterans associations, and they have done that recently, in the last 2 or 3 weeks.

Senator DUCKWORTH. Just a few weeks ago.

Mr. BARROS. Yes.

Senator DUCKWORTH. So was anything done? Mr. Smith, do you know? Was anything done when the breach was known and when it became public?

Mr. SMITH. Specific to the veterans?

Senator DUCKWORTH. Specific to government agencies in particular, but specifically to——

Mr. SMITH. Yes.

Senator DUCKWORTH.—agencies in particular, but specifically to the U.S. Department of Veterans Affairs and to the Department of Defense.

Mr. SMITH. Not that I'm aware of.

Senator DUCKWORTH. So you just left our veterans exposed.

Mr. SMITH. I'm saying not that I'm aware of.

Senator DUCKWORTH. Not that you're—well, I'd like to know. So please find out and provide me with that information.

Mr. SMITH. We'll do that.

Senator DUCKWORTH. So I want to be clear, the theft of VA disability benefits is an urgent problem that can be financially devastating for veterans who need these funds to pay their rent, to afford their groceries, and to keep the lights on. Even when a veteran notices that their disability benefit was not received, and contacts the VA, this merely represents a first step in what is an unacceptably complex and onerous bureaucratic maze that a veteran must navigate to get their disability benefits restored.

So as I understand it, this is what has to happen when a veteran discovers that, say, their disability check did not go into the bank account that it normally goes into. And thinking back to when this breach occurred, you'll see that veterans could still be suffering because you did not tell the VA, or hopefully you told them, but I—you have no evidence that you have.

First, the VA must confirm that with the financial institution, where the money was sent erroneously, that it received the information. Then the VA has to work out an agreement with that financial entity to return those funds back to the U.S. Treasury De-

partment's general fund. Then the VA must get a confirmation from the Treasury that the fraudulent payment was actually recouped, and then wait until Treasury actually returns the funds to VA before the VA will then send that money back to the veteran. In the best case scenario, this process can take weeks, but I wouldn't be surprised it would take many months.

Now, my office has warned various veteran service organizations of the need to notify their members of this danger. And I'm working with the VA to strengthen authentication policies and procedures. However, Mr. Barros, given your company's role in failing to safeguard this critical data, I would like Equifax's commitment to work with the VA, the veteran service organizations, and with individual veterans to provide valuable support and services, such as unlimited, free credit freezes, and monitoring for life. Will you make that commitment on behalf of the men and women who are willing to lay down their lives to protect you and your family and your business here in this country?

Mr. BARROS. We have, again, actually engaged with the Department of Defense and the veterans association, the Department of Veterans Affairs, and the CFPB, and the Senate. They will be offered the product that we have—they can use——

Senator DUCKWORTH. So you're not going to offer credit monitoring to all veterans who have been affected by your data breach for life?

Mr. BARROS. We're going to offer for them the lock and unlock product, which will provide the same barrier——

Senator DUCKWORTH. Again, again, as my colleague, Mr. Peters, just mentioned, that does not apply, that doesn't help, because the bad guys are going to go somewhere else. So basically you're saying that you will not make this commitment to our Nation's veterans.

Mr. BARROS. I have——

Senator DUCKWORTH. The people who protect your very ability to make money, who protect your freedoms, you will not support our veterans? Our disabled veterans who were wounded in their service to this country, you will not provide credit monitoring to them for life?

Mr. BARROS. We believe the lock and unlock product is a safer product than the monitoring that we have.

Senator DUCKWORTH. So the answer is no.

I'm overtime. I yield back, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Duckworth.

Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you so much, Chairman Thune, and thank you for holding this very important hearing. I must say some of the testimony is pretty discouraging here.

There were 846,188 New Mexicans whose identity and possibly their creditworthiness was endangered by the blatant carelessness of Equifax employees. When you previously testified, Mr. Smith, you specifically said that the data that was stolen was stored in plain text and had not been encrypted. This is an unacceptable practice for an organization with such power over consumers' lives.

And it's painfully clear that Americans cannot rely on large companies that store their data to protect it.

As one possible solution, Congress should consider banning the use of unverified Social Security numbers in commerce. There is the potential for strong bipartisan support for this. Social Security numbers were never intended to be used as universal online IDs. I'm glad to hear that the White House is looking at this idea, and Congress should also evaluate this possibility as well.

In that regard, this Committee should take a closer look at the work that the National Institute of Standards and Technology has initiated with the Trusted Identities Group to develop secure online IDs and to ban the use of unverified Social Security numbers. I look forward to working with others and building on the work this group has already undertaken.

The following are yes-or-no questions for all of the panelists. And I'm interested in banning the use of unverified Social Security numbers. Is it necessary for online commerce to rely on a Social Security number?

Mr. Barros.

[Pause.]

Senator UDALL. Please give me a yes or no. It's a simple question.

Mr. BARROS. The Social Security number was developed in 1936. I think we need to have a better digital identifier when dealing with e-commerce.

Senator UDALL. So your answer is yes, it's necessary to rely on it.

Mr. BARROS. Today, some sites do rely on it. It's not—in our case——

Senator UDALL. Mr. Smith?

Mr. SMITH. I'd love to see it replaced. Until there is a replacement, it's the standard.

Senator UDALL. Yes. Ms. Mayer?

Ms. MAYER. Yahoo! does not collect or store Social Security numbers, so we did not need it for the conduct of our business.

Senator UDALL. Yes.

Ms. ZACHARIA. Verizon is very happy to work with this Committee and others to come up with an alternative for Social Security numbers.

Senator UDALL. Thank you.

Mr. Wilkinson?

Mr. WILKINSON. Social Security numbers, a static identity, as a basis for our online identities, will not be secure, is not secure, and will never be secure in the future.

Senator UDALL. Do your businesses—another yes-or-no question—do your businesses require a consumer's Social Security number before you will do business with them?

Mr. BARROS. Most of our business is done business-to-business, so we deal mostly with entities.

Senator UDALL. So——

Mr. BARROS. It's just a small portion of our business that require information that there is on the consumer side.

Senator UDALL. Mr. Smith?

Mr. SMITH. I concur.

Senator UDALL. Ms. Mayer?
Ms. MAYER. No.
Senator UDALL. Ms. Zacharia?
Ms. ZACHARIA. The answer is no, but it is part of—it's not a requirement, but it is part of a typical way that we'll go through a credit check for a new customer.
Senator UDALL. Mr. Wilkinson?
Mr. WILKINSON. We're focused in the B2B area, and I don't collect consumer information and Social Security numbers.
Senator UDALL. Thank you.
Another question, do you think the development of a security digital ID could break the cycle of data breaches and identity theft?
Mr. BARROS. Yes.
Mr. SMITH. Yes.
Ms. MAYER. I think it's necessary, but not necessarily sufficient.
Senator UDALL. Ms. Zacharia.
Ms. ZACHARIA. Yes.
Mr. WILKINSON. Yes.
Senator UDALL. And the final one, Do you think it's worthwhile for Congress to consider legislation to restrict the use of unverified Social Security numbers and other personal information while promoting the use of secure digital identification?
Mr. BARROS. I need to understand the proposition, how it's going to be, but essentially anything that can move us forward from a static number, we'll be supportive.
Senator UDALL. OK. The same?
Mr. SMITH. I agree.
Senator UDALL. Yes. Ms. Mayer?
[No audible response.]
Senator UDALL. Yes. Just for the record, is that a yes or no?
Ms. MAYER. I don't know that my opinion matters, but yes.
Senator UDALL. Yes.
Ms. ZACHARIA. I agree.
Senator UDALL. Yes.
Mr. WILKINSON. Yes.
Senator UDALL. Mr. Wilkinson, yes.
The Trusted Identities Group is comprised of a public-private partnership to promote the adoption of an easy-to-use digital identity. And I'll just ask the final question here. I was wondering if you would work with this group. But since I'm running out of time here, will you commit to working with my office on ways to improve the current working group and expand its efforts?
Mr. BARROS. Definitely.
Senator UDALL. Thank you.
Mr. Smith.
[No audible response.]
Senator UDALL. Yes.
Ms. Mayer?
[No audible response.]
Senator UDALL. Yes.
Ms. Zacharia?
Ms. ZACHARIA. Absolutely.
Senator UDALL. Thank you. Thank you.
Mr. WILKINSON. Yes.

Senator UDALL. Thank you very much, Mr. Chairman. And I really appreciate you holding this hearing. I know that there was great interest on both sides of the aisle. And I think what I've seen today, I've been here for a long time listening today to the testimony, there are a lot of good ideas, and hopefully we can find a bipartisan way to really deal with a very tough situation.

Thank you very much.

The CHAIRMAN. Agreed. Thank you, Senator Udall.

My neighbor from Minnesota, Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Well, thank you very much, Mr. Chairman. And I thought, given that I'm the last one here to ask questions, I would use this opportunity to welcome Mr. Wilkinson. I hope things have been going well from my home state here before us again. And Entrust Datacard employs more than 2,200 workers worldwide, and 800 of them in our state. So thank you for being here.

So I'll start with you. And I know much of this ground has been covered, but not this exact question. In your testimony, you mentioned Brazil's model of issuing dynamic identities to citizens. And in this model, the government partners with industry to provide consumers options to access digital certificates for identification. How do they ensure that the government's private partners can keep citizens' information safe?

Mr. WILKINSON. So some of the models that—you know, Brazil is a great example, but there are certain models, Senator, that we can share with you that are being used around the world that I wouldn't necessarily promote in the U.S. in terms of, you know, where the center of the trusted identity lies. But certainly the framework that they've built for secure identity is one that's very close to what we're proposing in terms of looking forward to the framework for a secure identity going forward.

The comment Senator Udall made just a few moments ago talking about NIST and the work that they're doing with the Trusted Identities Group is one that we follow very closely. And they're actually also doing really good work that we would love to spend more time with the Committee speaking about and helping to describe what security identity could look like in the future.

Senator KLOBUCHAR. OK. Thank you very much.

Mr. Smith appeared before us in Judiciary, and I think I expressed my—the shared frustration I have with others in the Senate about what went on.

But I thought I would focus with you, Mr. Barros, on what's happening now. So Equifax has announced that it would be launching this app—right?—in January that will allow consumers to lock and unlock personal credit data while providing consumers with more control over their credit information is a positive step. We don't want to have new avenues for hackers. So are there additional cybersecurity challenges that come with this mobile technology? And how is the product going to be tested?

Mr. BARROS. The product is being developed as we speak. We are on time to deliver this in January. One of the advantages of the

system is the simplicity and how consumers can actually understand and use the application to do that. We just started our development tests now. And this is a straight connection to our main files, so it has all the security needs and requirements that will make the product be in compliance with security.

Senator KLOBUCHAR. OK. I've been working a lot, of course, on the election issue, since I'm the Ranking on Rules, and we've been really concerned. Senator Graham and I have a bill to upgrade our election equipment when we had attempts to hack 21 state elections equipment, manufacturers, or software companies. And so I see this as kind of going hand-in-hand with the attacks I've seen on some of my companies, like Target and other places.

Ms. Mayer, you know, we have individual hackers, and then we also have these state-sponsored attacks, like what we believe occurred in the 2016 election. So in your experience at Yahoo!, how do state-sponsored attacks differ from those committed by individual hackers?

Ms. MAYER. In many cases, the motivation is different. And I would also say that they tend to be much more sophisticated, much more——

Senator KLOBUCHAR. The state-sponsored.

Ms. MAYER. The state-sponsored tend to be much more sophisticated, persistent, they last for longer periods of time, they attack more targets. And they span over often several companies trying to stitch together a picture of what they're actually seeking, and they are very good at hiding their tracks.

The four people indicted in the case with Yahoo!, one of them, Alexsey Belan, is considered to be perhaps the most sophisticated and dangerous hacker in the world today, and he's a central figure in many of these ongoing investigations. But when you're that empowered, well-funded, motivated, and sophisticated to work such a complex campaign, especially across multiple targets and sources, it's an issue.

Senator KLOBUCHAR. So what do you think we could be doing differently for those kinds of state-sponsored attacks? What should we be doing out of Congress, when you look at the whole scope of things, the business, the government, the election equipment?

Ms. MAYER. I think that really aggressive pursuit of the hacking is important. And I was really pleased with the FBI and Department of Justice's work with Yahoo! to bring the people who perpetrated the crimes against us to justice. And I think that we should be empowering them legislatively and financially to pursue hacking because right now there is just not enough of a disincentive to hack either on a commercial or criminal level or a state-sponsored level.

Senator KLOBUCHAR. And these would be international cases, a lot of them obviously, and then they could involve sanctions or other things if we find that. But that's what you're talking about, much more aggressive about going after these in addition to doing everything we can to protect the software.

Ms. MAYER. Yes. And one of the individuals in the Yahoo! case was apprehended in Canada and has been extradited to the U.S.

Senator KLOBUCHAR. Mm-hmm. Good example. And I think on the election side, you know, it's different. We have to get backup

paper ballots. It's a one-time occurrence, but it is a lot of the same issues that business is facing as well.

So thank you very much.

Thank you.

The CHAIRMAN. Thank you, Senator Klobuchar.

I think we—you guys made it through.

We will keep the record open, and we'll allow Members to submit questions for the record for a couple of weeks, but we will want to close it out. So if you could respond as quickly as you can in writing to the questions that the members of this Committee submit, we'll get them included in the record.

And, again, I appreciate all of you being here today. I think this has shed a lot of light on this subject. And as was mentioned earlier by a number of the members on both sides of this Committee, we have an interest in moving forward on the legislative front in a way hopefully that will be effective in helping to prevent these types of cyber attacks in the future.

So thank you again. And with that, this hearing is adjourned.

[Whereupon, at 12:31 p.m., the hearing was adjourned.]

A P P E N D I X

For Immediate Release
November 3, 2017

EQUIFAX BOARD RELEASES FINDINGS OF SPECIAL COMMITTEE REGARDING STOCK SALE BY EXECUTIVES

Review Concludes Executives Acted Appropriately

ATLANTA. Nov. 3, 2017 -- The Board of Directors of Equifax Inc. (NYSE: EFX) today released a report by the Special Committee regarding the trading of Company securities by certain executives following the detection by Equifax cybersecurity personnel of suspicious activity in the Company's network and prior to public disclosure of the incident. The Board formed the Special Committee in September to conduct an independent review of various aspects of the cybersecurity incident and the Company's response to it. The report released today relates exclusively to the securities trading matter.

The Special Committee's report, which is attached, concludes that "none of the four executives had knowledge of the incident when their trades were made, that preclearance for the four trades was appropriately obtained, that each of the four trades at issue comported with Company policy, and that none of the four executives engaged in insider trading." As part of the review process, the Special Committee conducted dozens of interviews, and reviewed more than 55,000 documents including emails, text messages, phone logs and other records.

"I'm grateful for the timely and thorough review by the Special Committee of this important matter. The Board takes very seriously any allegation of insider trading. It is critically important for the public, our shareholders, our customers and our employees to know that we will not tolerate any violation of Company policy or the law regarding the trading of securities. The conclusion that the Company executives in question traded appropriately is an extremely important finding and very reassuring," said Non-Executive Chairman Mark L. Feidler.

The Special Committee of the Board is comprised of independent directors and is advised by independent counsel. The Special Committee continues to review the cybersecurity incident, the Company's response to it, and all relevant policies and practices.

ABOUT EQUIFAX

Equifax is a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions. Headquartered in Atlanta, Ga., Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX. Equifax employs approximately 10,100 employees worldwide.

Contact:
Marisa Salcines, Media Relations
mediainquiries@equifax.com

REPORT OF THE SPECIAL COMMITTEE OF

THE BOARD OF DIRECTORS OF EQUIFAX INC.

Elane B. Stock, Chair

Robert D. Daleo

G. Thomas Hough

November 1, 2017

Counsel
Wilmer Cutler Pickering Hale and Dorr LLP

REPORT OF THE SPECIAL COMMITTEE

In September 2017, the Board of Directors of Equifax Inc. formed a Special Committee of independent directors to address matters related to the cybersecurity incident disclosed by Equifax on September 7, 2017. The Special Committee was charged with conducting an independent review of the circumstances of trading in Equifax securities by certain executives following the discovery by Equifax of suspicious activity on its network and prior to the public disclosure of the incident. The Special Committee was advised by Wilmer Cutler Pickering Hale and Dorr LLP ("WilmerHale") in conducting the review, and the Special Committee directed WilmerHale during the course of the investigation. This report presents the findings of the Special Committee and the work of WilmerHale resulting from the review of the trading.

Equifax has an Insider Trading Policy applicable to all employees. Under that policy, no employee may trade in Equifax securities if he or she possesses material non-public information regarding Equifax. In addition, Equifax directors and certain senior Equifax officers may trade in Equifax securities only in specified "trading windows" and only if they first receive preclearance by the Equifax Chief Legal Officer or his designee.

Four senior officers at Equifax who are subject to this trading preclearance requirement sought and received preclearance to sell shares in Equifax securities between July 28 and August 1, 2017. Those officers are John W. Gamble, Jr. (Chief Financial Officer), Joseph M. ("Trey") Loughran, III (President, U.S. Information Solutions), Rodolfo O. ("Rudy") Ploder (President, Workforce Solutions), and Douglas G. Brandberg (Senior Vice President, Investor Relations). Equifax identified some suspicious activity on its network on the evening of Saturday, July 29, and Equifax personnel immediately began to assess the activity.

The Special Committee examined whether the trades of those officers comported with the Company's Insider Trading Policy, whether the executives had any information about the security incident when they made their trades, and whether preclearance was appropriately obtained.[1]

For the reasons set out below, the Special Committee has determined that none of the four executives had knowledge of the incident when their trades were made, that preclearance for the four trades was appropriately obtained, that each of the four trades at issue comported with Company policy, and that none of the four executives engaged in insider trading.

METHODOLOGY

The Special Committee's review examined the circumstances under which Equifax identified suspicious activity on its network, and the review was designed to pinpoint the date on

[1] Initially, the Special Committee focused on the three officers of Equifax (Messrs. Gamble, Loughran, and Ploder) who sold shares during the period under review and who are Section 16 officers of the Company, *i.e.*, covered by Rule 16a-1(f) under Section 16 of the Securities Exchange Act on 1934. The Committee thereafter determined to expand the review to cover all officers of the company – whether covered by Section 16 or not – who required pre-clearance for trading in Equifax shares under the Company's Insider Trading Policy and who sold shares during the relevant period. This change led to the inclusion of Mr. Brandberg in the review.

which each of the four senior officers first learned of the security investigation that uncovered the breach and to determine whether any of those officers was informed of or otherwise learned of the security investigation before his trades were executed. The review also entailed analysis of the Company's Insider Trading Policy as applied to these four trades.

The Special Committee conducted an extensive review of documents and communications during the period surrounding the four officers' trading in Equifax securities. The Special Committee also conducted dozens of interviews with individuals involved in or knowledgeable about the security investigation and/or the trade preclearance process in the relevant period. Finally, the Special Committee conducted lengthy in-person interviews with each of the four senior officers who executed trades. In conducting its review, the Special Committee received full cooperation from all Equifax employees including from the four senior officers, who supplied all requested information.

Document Review. The Special Committee reviewed over 55,000 documents, comprising emails, text messages, phone logs, and other records:

- As to each of the four senior officers, the Committee reviewed all of their Equifax emails, texts, calendars, voicemails, phone logs, and electronic documents, along with all Equifax emails and texts of each of their administrative assistants, for the period July 29 through August 2, 2017.[2] For the period of August 3 through September 7 (when the incident was announced publicly), the Committee conducted a targeted review of their Equifax communications, using search terms designed to identify documents concerning the incident or trading. The Committee also reviewed relevant materials from their personal emails, texts, phone logs, and other documents. Finally, the Committee reviewed documents related to the officers' Equifax holdings and trading history.

- As to employees in the Equifax Legal Department most involved in the security investigation and/or the preclearance of the trades at issue, and for Equifax's then-Chief Security Officer, the Committee reviewed all Equifax emails, texts, voicemails, calendars, and other electronic documents for the period of July 29 through August 2. The Committee also conducted a targeted review of their emails from August 3 through September 7, using search terms to identify documents concerning trading.

- As to all Equifax employees identified as having knowledge of the security investigation on or prior to the dates of the trades at issue, the Committee conducted a targeted review of Equifax emails in the period July 29 through August 2, using search terms to identify documents concerning the four officers

[2] This period spans the Company's detection of suspicious activity on the network through the date on which the last of the senior officer's securities transactions were executed.

and, where feasible, a full review of Equifax text messages from the period July 29 through September 7.[3]

Interviews. The Special Committee conducted 62 interviews, including lengthy in-person interviews with each of the four senior officers. During those interviews, the Committee addressed the officers' trading history, documents and recollections surrounding the August 2017 trades, and knowledge of the security investigation that uncovered the breach. The Committee also interviewed, in person or telephonically, each current or former Equifax employee identified as potentially possessing knowledge of the security investigation on or before the date on which the senior officers conducted their trades. During those interviews, the Committee sought to determine whether the employee had contact with any of the four officers during that period, and if so, whether that contact included any discussion of the security investigation then underway.

FINDINGS

The Special Committee found the following concerning the trading by each of the four senior officers:

John Gamble. As is standard under the Company's Insider Trading Policy, Mr. Gamble received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Gamble and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Gamble traveled to Utah with his wife on July 28 on non-Equifax business. On July 31, while in Utah, Mr. Gamble sent an email to the Legal Department requesting preclearance to sell 6,500 shares of Equifax stock (approximately 13.4% of his holdings at the time). Mr. Gamble's Equifax share grants had recently started to vest, and he had previously discussed with his financial adviser his goals to diversify his assets and to pay for an ongoing home renovation. Mr. Gamble's request to trade was approved via email on July 31, and the trade was executed on August 1.

Nine days after Mr. Gamble's trade, on August 10, during a management offsite meeting, Mr. Gamble first learned of the existence of a security incident at Equifax that was under investigation. Mr. Gamble received a more detailed briefing the following week, on August 17, and received additional details of the incident on August 22, during a Senior Leadership Team meeting.

[3] On August 15, 2017, the Equifax Legal Department imposed a trading blackout on all company personnel identified as aware of the breach as of that date. The Special Committee used the recipient list for the August 15 blackout notice to isolate the initial population of Equifax employees whose documents and communications should be reviewed. To the extent additional individuals were identified as potentially knowledgeable about the breach investigation during the Committee's review, their emails and texts were subject the same process, and those persons were interviewed.

The Special Committee concluded that Mr. Gamble did not have any knowledge of the security incident when he sought preclearance to trade on July 31 or when he executed his cleared trades on August 1. The Special Committee further concluded that Mr. Gamble fully complied with Company policy and did not engage in insider trading.

Trey Loughran: As is standard under the Company's Insider Trading Policy, Mr. Loughran received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Loughran and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Loughran sent an email to the Legal Department requesting preclearance to sell Equifax securities on July 28, 2017, one day before suspicious activity on the network was identified. On July 31, in response to a request from the Legal Department for greater specificity regarding the number and type of shares he wanted to sell, Mr. Loughran clarified that his request was to sell 4,000 shares (approximately 9.4% of his holdings at the time). Mr. Loughran's request for preclearance was approved on July 31, and the sale occurred on August 1. Mr. Loughran's sale of Equifax securities was consistent with previous sales he had made and was part of an effort to diversify his holdings.

Mr. Loughran first learned, at a general level, that a security issue was being investigated in a series of texts, emails, and phone calls he exchanged with members of the Equifax Legal Department on August 13 and 15. Mr. Loughran learned details of the breach on August 22, when he attended the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Loughran did not have any knowledge of the security incident when he sought preclearance to trade on July 28 or when he executed his cleared trades on August 1. The Special Committee further concluded that Mr. Loughran fully complied with Company policy and did not engage in insider trading.

Rudy Ploder: As is standard under the Company's Insider Trading Policy, Mr. Ploder received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Ploder and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Ploder sent an email to the Legal Department requesting preclearance to sell Equifax securities on August 1. Preclearance was granted that same day, and his trade executed on August 2. Mr. Ploder sold 1,719 shares (approximately 3.8% of his holdings at the time). Mr. Ploder's trade was motivated by, among other things, a need to meet costs associated with a business-related move to St. Louis and was consistent with his previous sales of Equifax shares.

Mr. Ploder learned of the security incident on August 22, 2017, when he participated in the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Ploder did not have any knowledge of the security incident when he sought preclearance to trade on August 1 or when he executed his cleared trades on August 2. The Special Committee further concluded that Mr. Ploder fully complied with Company policy and did not engage in insider trading.

Douglas Brandberg: As is standard under the Company's Insider Trading Policy, Mr. Brandberg received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Brandberg and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Brandberg sent an email to the Legal Department requesting preclearance to sell Equifax securities on August 1, 2017. Preclearance was granted on August 1, and his trade was executed on August 2. Mr. Brandberg sold 1,724 shares. Mr. Brandberg's sale of Equifax securities was consistent with his previous practice of selling shares as they vested; his sale was driven by family expenses.

Mr. Brandberg first learned that a security issue was being investigated on approximately August 14, and learned details of the security incident on August 22, when he attended the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Brandberg did not have any knowledge of the security incident when he sought preclearance to trade on August 1 or when he executed his cleared trades on August 2. The Special Committee further concluded that Mr. Brandberg fully complied with Company policy and did not engage in insider trading.

The Application of the Insider Trading Policy. Messrs. Gamble, Loughran, Ploder, and Brandberg each sought and received clearance from the appropriate Legal Department personnel prior to trading. Based on its review, the Committee has concluded that neither Equifax's Chief Legal Officer nor his designated preclearance officer had reason to believe that Messrs. Gamble, Loughran, Ploder, or Brandberg had knowledge of the security incident's existence as of the date of their preclearance requests or the date of their trades. Accordingly, the Special Committee has concluded that the preclearance authorization obtained by Messrs. Gamble, Loughran, Ploder, and Brandberg was within the authority permitted under the policy.

* * *

The Special Committee continues to review the cybersecurity incident, the Company's response to it, and all relevant policies and practices.

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org
National Association of Federally-Insured Credit Unions

November 7, 2017

The Honorable John Thune
Chairman
Committee on Commerce, Science,
& Transportation
United States Senate
Washington, D.C. 20510

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science,
& Transportation
United States Senate
Washington, D.C. 20510

Re: Tomorrow's Hearing "Protecting Consumers in the Era of Major Data Breaches"

Dear Chairman Thune and Ranking Member Nelson:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today in conjunction with tomorrow's hearing, "Protecting Consumers in the Era of Major Data Breaches." We appreciate the Committee's continued focus on the Equifax data breach and the need for addressing consumer data security issues. As NAFCU has previously communicated to the Committee, there is a need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements as depository institutions.

Unfortunately, data breaches have become a constant concern of the American people. Major data breaches now occur with an unacceptable level of regularity. A recent Gallup poll found that 69 percent of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers. These staggering survey results speak for themselves and should demonstrate the need for greater national attention to this issue.

While credit reporting agencies, such as Equifax, are governed by data security standards set forth by the *Gramm-Leach-Bliley Act* (GLBA), they are not examined by a regulator for compliance with these standards in the same manner as depository institutions. Additionally, the recent Equifax breach reportedly occurred through a "known" security vulnerability that software companies had issued a patch to fix several weeks prior. If Equifax had acted to remedy the vulnerability in a reasonable period of time, this breach may not have occurred. When a breached entity knew or should have known about a threat, and fails to act to mitigate it, the negligent company must be held financially liable.

Credit unions suffer steep losses in re-establishing member safety after a data breach like the one at Equifax and are often forced to absorb fraud-related losses in its wake. Credit unions and their members are victims in this breach, as members turn to their credit union for answers and

support when such breaches occur. As not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

Negligent entities should be held financially liable for any losses that occurred due to breaches on their end so that consumers aren't left holding the bag. When a breach occurs at a credit bureau, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts. Furthermore, compliance by credit bureaus with GLBA and these notification requirements should be examined for, and enforced by, a federal regulator. Finally, any new rules or regulations to implement these recommendations should recognize credit unions' compliance with GLBA and not place any new burdens on them.

On behalf of our nation's credit unions and their more than 110 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information please contact me or Chad Adams, NAFCU's Senior Associate Director of Legislative Affairs, at 703-842-2265 or cadams@nafcu.org.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Committee on Commerce, Science, and Transportation

NRF
THE VOICE OF RETAIL

November 8, 2017

The Honorable John Thune
Chairman, Committee on Commerce,
Science, and Transportation
United States Senate
Washington, DC 20510

The Honorable Bill Nelson
Ranking Member, Committee on Commerce
Science, and Transportation
United States Senate
Washington, DC 20510

RE: Hearing on Protecting Consumers in the Era of Major Data Breaches

Dear Chairman Thune and Ranking Member Nelson:

The National Retail Federation applauds your holding of today's hearing to review the recent breaches of data security at Equifax and Yahoo that have collectively affected billions of consumers globally, and hundreds of millions of American citizens. Consumers in the United States did not receive clear and timely notice of theses breaches and, in the case of Yahoo, did not learn of some of their recently reported breaches for years. Similarly, financial institutions and third-party service providers have sought to maintain exemptions in breach legislation that permit them to keep the fact of their own breaches secret. For over a decade, NRF has supported, and worked with members of this Committee to craft, federal data security legislation that would create a uniform, national requirement for *all* breached businesses to provide notice of their breaches to affected individuals.

By way of background, NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

According to the 2017 Verizon Data Breach Investigations Report, all sectors of U.S. industry are affected by security breaches, but three collectively account for the majority of all breaches, defined as security incidents with confirmed data loss. Verizon reported that the financial services sector had 24.3% of all breaches last year, while the healthcare sector accounted for 15.3% and the public sector (e.g., governmental entities) had 12.4%. Not surprisingly, these sectors also handle American's most sensitive personal information, and the hackers know this. By contrast, businesses with less sensitive data generally account for fewer breaches. Verizon reported, for instance, that the retail industry suffered just 4.8% of all breaches last year. The bottom line is that all entities that handle consumers' personal information, whether they do so through direct contact with customers or as third parties, face security threats that put at risk any sensitive data in their possession. To protect customers comprehensively, federal laws must apply to *all* sectors and leave no holes for some industries that hackers can exploit.

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

Some federal breach bills under consideration contain "notice holes" – exemptions from the legislation's breach notice provisions altogether, or special provisions that permit some types of businesses to shift their breach notice obligations onto others. The companies testifying today would enjoy exemptions in leading House breach legislation under both scenarios. For example, under the breach legislation reported by the House Financial Services Committee last Congress, Equifax is exempt from the bill's provisions, as are banks, credit unions and other entities that qualify as "financial institutions" under the Gramm Leach Bliley Act (GLBA). Enacted in 1999, however, GLBA *predates* the first state breach notification law by four years, and consequently it contains no statutory requirement for breached financial institutions to notify affected individuals of their breaches. Furthermore, the regulatory guidance issued under GLBA merely states that financial institutions "should" notify affected individuals following a breach, not "must." Not surprisingly, banks, credit unions and the broader financial services sector only support federal breach legislation that would preserve this notice hole by exempting GLBA-covered entities from any requirements to notify consumers affected by a breach.

Under the second scenario, special breach notice provisions would actually *permit* these breached businesses to shift the obligation to notify affected consumers of their own breach onto the unbreached businesses they serve. Verizon, for instance, only supports breach legislation where it qualifies as a "service provider" and enjoys special notice exemptions, such as in the bills reported by both the House Financial Services Committee and House Energy & Commerce Committee. Under these bills, qualifying service providers are *not* required to make notice of their *own* breaches. In some circumstances under these bills, they can even be aware of a breach of their own network and not be required to make notice of the breach to anyone at all – not to affected consumers, not to affected businesses, and not to government enforcement authorities. In other circumstances, qualifying service providers can simply shift the obligation to notify affected consumers onto the businesses they serve. This special treatment, which amounts to a notice hole for ISPs, is unjustified, particularly when consumers are affected by breaches wherever they occur.

As this Committee considers federal breach legislation in the wake of the Equifax and Yahoo breaches, we urge you to avoid the flaws in previous attempts at federal legislation by closing the notice holes that would permit financial institutions and service providers to avoid making notice of their breaches. We look forward to working with you and the members of the Committee to enact federal data breach legislation that establishes a uniform breach notification standard so that all Americans will be notified by businesses that have suffered a breach of security affecting their sensitive personal information.

Sincerely,

David French
Senior Vice President
Government Relations

cc: The Honorable Mitch McConnell
The Honorable Chuck Schumer
Members of the Senate Commerce Committee

quinn emanuel trial lawyers | washington, dc
777 Sixth Street NW, 11th Floor, Washington, District of Columbia 20001-3706 | TEL (202) 538-8000 FAX (202) 538-8100

WRITER'S DIRECT DIAL NO.
(213) 443 3150

WRITER'S EMAIL ADDRESS
stevemadison@quinnemanuel.com

November 17, 2017

VIA US MAIL AND EMAIL

The Honorable John Thune, Chairman
U.S. Senate Committee on Commerce,
Science, and Transportation
Washington, DC 20510

The Honorable Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce,
Science, and Transportation
Washington, DC 20510

Re: *Richard F. Smith Congressional Hearing Testimony*

Dear Chairman Thune and Ranking Member Nelson:

We write further to the appearance by Richard F. Smith at the November 8 hearing before the U.S. Senate Committee on Commerce, Science, and Transportation, "Protecting Consumers in the Era of Major Data Breaches."

In response to a question from Senator Young concerning Mr. Smith's compensation, Mr. Smith stated he was retiring from Equifax with his pension. Specifically, he replied:

> I understand your point, Senator, but as I said in prior testimonies, I've left with nothing except the pension. I've asked for nothing. I waived my bonus, there's no equity coming next year, I've worked for three months to six months, as long as needed, for free in an advisory capacity . . . . What I'm walking away with was all disclosed in the proxy is my pension.

Protecting Consumers in the Era of Major Data Breaches: Hearing Before the S. Comm. on Commerce, Sci., and Transp., 115th Cong. 106 (2017) (statement of Richard Smith).

To clarify and amplify, as Mr. Smith has previously testified, he retired from Equifax with both a pension and certain unvested equity previously earned, as disclosed in Equifax's proxy statement. Specifically, on October 4, 2017, Mr. Smith testified before the Senate Banking Committee, "What I walk away with is a pension that I've earned over my career and unvested equity that was given to me . . . . The pension, Senator, is something I've earned for my career. And the other piece is the earned equity I've already been given." *An Examination of the Equifax Cybersecurity Breach: Hearing Before the S. Comm. on Banking, Hous., and Urban Affairs,*

115th Cong. 35 (2017) (statement of Richard Smith). The next day, Mr. Smith testified before the House Financial Services Committee, "I asked for nothing beyond what was disclosed in the proxy, and that is a pension that I've accumulated over my career. And that is some equity that I've earned in the past." *Examining the Equifax Data Breach: Hearing Before the H. Comm. on Fin. Serv.*, 115th Cong. 45–46 (2017) (statement of Richard Smith).

We respectfully request that this letter be made part of the record of the November 8 hearing. If any further information is needed, please let us know. Thank you.

Very truly yours,

Steven G. Madison

cc Hon. Todd Young

KING & SPALDING

King & Spalding LLP
1700 Pennsylvania Ave, NW
Washington, D.C. 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
www.kslaw.com

Theodore M. Hester
Direct Dial: 202-626-2901
thester@kslaw.com

VIA E-MAIL

December 19, 2017

Confidential Treatment Requested

The Honorable John Thune
Chairman
Committee on Commerce, Science, and
Transportation
United States Senate
512 Dirksen Senate Building
Washington, D.C. 20510

RE: Equifax's Recommendations for Testimony Corrections and Responses to Questions for the Record

Dear Chairman Thune:

On behalf of our client, Equifax Inc. ("Equifax" or "Company"), I am writing in response to emails from Committee staff dated November 22 and 29, 2017 regarding Equifax's November 8, 2017 testimony before the Committee on Commerce, Science, and Transportation ("Committee") and related questions for the record. This response supplements Equifax's submissions to the Committee dated September 25, 2017 and October 6, 2017.

Additionally, Mr. Paulino do Rego Barros, Jr has asked me to submit the proposed corrections to the transcript of his testimony from the November 8, 2017 hearing before the Committee, and to provide clarifications to certain responses he provided at the hearing (see attached Appendix A). We respectfully request that Mr. Barros's clarifications be included in the hearing record. Furthermore, Equifax has asked me to formally submit the enclosed information in response to the Committee's questions for the record (see attached Appendix B).

This letter and the information enclosed may contain or constitute confidential, trade secret, and proprietary information of Equifax provided pursuant to the Committee's requests. Accordingly, Equifax has marked all documents produced today with the legend "CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC."

In responding to the Committee's questions at the November 8 hearing, Mr. Barros used his best efforts to be as accurate and responsive as possible based on his knowledge and recollection of the facts. Similarly, in submitting the requested edits to the hearing transcript and information in response to the Committee's subsequent questions for the record, Equifax has used its best efforts to be as accurate and responsive as possible within the time frame set by the Committee and the Company's understanding of the terms used in the Committee's requests. The representations herein are based on reasonably available information and are not intended to, and do not, capture every event related to Equifax's ongoing investigation, nor are they an exhaustive description of the events discussed.

In providing information in response to the Committee's questions for the record, the Company does not waive, nor does it intend to waive, any of its rights or privileges with respect to this inquiry by the Committee, including any applicable attorney-client, work product, or other evidentiary privilege, or any objection to the letter request from the Committee. We respectfully request advance notice of any contemplated disclosure of the Company's confidential, trade secret, and proprietary information, and a reasonable opportunity to object. Please direct any such notice to me at the above address.

Should you have any questions concerning the information provided herein, please contact me directly at 202-626-2901.

Sincerely,

Theodore M. Hester

cc: The Honorable Bill Nelson, Ranking Member

Enclosures

Appendix A

CLARIFICATIONS TO THE TESTIMONY OF PAULINO DO REGO BARROS, JR. AT THE NOVEMBER 8, 2017 HEARING OF THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Senator Brian Schatz asked whether an individual who receives a credit report from Equifax is able to see the same information that a financial institution receives from Equifax when it evaluates that consumer's creditworthiness. To clarify Mr. Barros's response, when a consumer receives a copy of his or her credit report from Equifax Information Services LLC ("EIS"), the consumer receives all information EIS has on that consumer, which includes information provided by EIS to banks. That said, many banks rely on their own specific credit score when evaluating a consumer's creditworthiness. In other words, although individuals can obtain educational credit scores from Equifax, the particular scores that the banks calculate and utilize are not available to individual consumers from EIS.

Senator Moran asked how much Equifax was spending to prevent a future cybersecurity incident. Mr. Barros testified that Equifax was spending significantly more to prevent future incidents. In response to further questioning from Senator Moran, Mr. Barros stated that he believed Equifax was spending "four times" more to prevent a future breach. To clarify that answer, security experts recommend—and the industry has generally adopted as a standard—that a company should dedicate 10–14% of its information technology ("IT") budget to security. Equifax has historically spent within that range. Since the cybersecurity incident, Equifax has spent considerably more than that standard to harden security, and expects that spike in investment to continue for a period of time.

Senator Baldwin asked Mr. Barros if he had any information about who hacked Equifax and possesses the personal identifying information that was stolen from the Company. Mr. Barros answered that Equifax had "no evidence." Mr. Barros' answer was accurate; Equifax is not aware of evidence sufficient to attribute responsibility for the breach. Equifax has shared evidence with law enforcement for the investigation of the criminal conduct and continues to cooperate with the FBI's investigation into the incident.

In response to questions from Senators Capito and Gardner, Mr. Barros stated that nobody can have access to the information in an individual's locked credit file. To clarify that answer, locking an Equifax credit file will prevent access to a consumer's Equifax credit file by certain third parties. Locking the Equifax credit file will not prevent access to the consumer's credit file maintained by other credit reporting agencies. Entities that may still have access to a consumer's locked Equifax credit file include companies like Equifax Global Consumer Solutions, which provide consumers with access to their credit report or credit score, or monitor the consumer's credit file; federal, state, and local government agencies; companies reviewing a consumer's application for employment; companies that have a current account or relationship with the consumer, and collection agencies acting on behalf of those to whom a consumer owes debt; companies utilizing the information for fraud prevention and detection purposes; and companies that make pre-approved offers of credit or insurance to the consumer. Consumers can opt out of pre-approved offers at www.optoutprescreen.com. Similarly, under state freeze laws

certain third parties, like those mentioned above, may continue to have access to a frozen Equifax credit file.

REPORT OF THE SPECIAL COMMITTEE OF

THE BOARD OF DIRECTORS OF EQUIFAX INC.

Elane B. Stock, Chair

Robert D. Daleo

G. Thomas Hough

November 1, 2017

Counsel
Wilmer Cutler Pickering Hale and Dorr LLP

REPORT OF THE SPECIAL COMMITTEE

In September 2017, the Board of Directors of Equifax Inc. formed a Special Committee of independent directors to address matters related to the cybersecurity incident disclosed by Equifax on September 7, 2017. The Special Committee was charged with conducting an independent review of the circumstances of trading in Equifax securities by certain executives following the discovery by Equifax of suspicious activity on its network and prior to the public disclosure of the incident. The Special Committee was advised by Wilmer Cutler Pickering Hale and Dorr LLP ("WilmerHale") in conducting the review, and the Special Committee directed WilmerHale during the course of the investigation. This report presents the findings of the Special Committee and the work of WilmerHale resulting from the review of the trading.

Equifax has an Insider Trading Policy applicable to all employees. Under that policy, no employee may trade in Equifax securities if he or she possesses material non-public information regarding Equifax. In addition, Equifax directors and certain senior Equifax officers may trade in Equifax securities only in specified "trading windows" and only if they first receive preclearance by the Equifax Chief Legal Officer or his designee.

Four senior officers at Equifax who are subject to this trading preclearance requirement sought and received preclearance to sell shares in Equifax securities between July 28 and August 1, 2017. Those officers are John W. Gamble, Jr. (Chief Financial Officer), Joseph M. ("Trey") Loughran, III (President, U.S. Information Solutions), Rodolfo O. ("Rudy") Ploder (President, Workforce Solutions), and Douglas G. Brandberg (Senior Vice President, Investor Relations). Equifax identified some suspicious activity on its network on the evening of Saturday, July 29, and Equifax personnel immediately began to assess the activity.

The Special Committee examined whether the trades of those officers comported with the Company's Insider Trading Policy, whether the executives had any information about the security incident when they made their trades, and whether preclearance was appropriately obtained.[1]

For the reasons set out below, the Special Committee has determined that none of the four executives had knowledge of the incident when their trades were made, that preclearance for the four trades was appropriately obtained, that each of the four trades at issue comported with Company policy, and that none of the four executives engaged in insider trading.

METHODOLOGY

The Special Committee's review examined the circumstances under which Equifax identified suspicious activity on its network, and the review was designed to pinpoint the date on

[1] Initially, the Special Committee focused on the three officers of Equifax (Messrs. Gamble, Loughran, and Ploder) who sold shares during the period under review and who are Section 16 officers of the Company, *i.e.*, covered by Rule 16a-1(f) under Section 16 of the Securities Exchange Act on 1934. The Committee thereafter determined to expand the review to cover all officers of the company – whether covered by Section 16 or not – who required pre-clearance for trading in Equifax shares under the Company's Insider Trading Policy and who sold shares during the relevant period. This change led to the inclusion of Mr. Brandberg in the review.

which each of the four senior officers first learned of the security investigation that uncovered the breach and to determine whether any of those officers was informed of or otherwise learned of the security investigation before his trades were executed. The review also entailed analysis of the Company's Insider Trading Policy as applied to these four trades.

The Special Committee conducted an extensive review of documents and communications during the period surrounding the four officers' trading in Equifax securities. The Special Committee also conducted dozens of interviews with individuals involved in or knowledgeable about the security investigation and/or the trade preclearance process in the relevant period. Finally, the Special Committee conducted lengthy in-person interviews with each of the four senior officers who executed trades. In conducting its review, the Special Committee received full cooperation from all Equifax employees including from the four senior officers, who supplied all requested information.

Document Review. The Special Committee reviewed over 55,000 documents, comprising emails, text messages, phone logs, and other records:

- As to each of the four senior officers, the Committee reviewed all of their Equifax emails, texts, calendars, voicemails, phone logs, and electronic documents, along with all Equifax emails and texts of each of their administrative assistants, for the period July 29 through August 2, 2017.[2] For the period of August 3 through September 7 (when the incident was announced publicly), the Committee conducted a targeted review of their Equifax communications, using search terms designed to identify documents concerning the incident or trading. The Committee also reviewed relevant materials from their personal emails, texts, phone logs, and other documents. Finally, the Committee reviewed documents related to the officers' Equifax holdings and trading history.

- As to employees in the Equifax Legal Department most involved in the security investigation and/or the preclearance of the trades at issue, and for Equifax's then-Chief Security Officer, the Committee reviewed all Equifax emails, texts, voicemails, calendars, and other electronic documents for the period of July 29 through August 2. The Committee also conducted a targeted review of their emails from August 3 through September 7, using search terms to identify documents concerning trading.

- As to all Equifax employees identified as having knowledge of the security investigation on or prior to the dates of the trades at issue, the Committee conducted a targeted review of Equifax emails in the period July 29 through August 2, using search terms to identify documents concerning the four officers

[2] This period spans the Company's detection of suspicious activity on the network through the date on which the last of the senior officer's securities transactions were executed.

and, where feasible, a full review of Equifax text messages from the period July 29 through September 7.[3]

Interviews. The Special Committee conducted 62 interviews, including lengthy in-person interviews with each of the four senior officers. During those interviews, the Committee addressed the officers' trading history, documents and recollections surrounding the August 2017 trades, and knowledge of the security investigation that uncovered the breach. The Committee also interviewed, in person or telephonically, each current or former Equifax employee identified as potentially possessing knowledge of the security investigation on or before the date on which the senior officers conducted their trades. During those interviews, the Committee sought to determine whether the employee had contact with any of the four officers during that period, and if so, whether that contact included any discussion of the security investigation then underway.

FINDINGS

The Special Committee found the following concerning the trading by each of the four senior officers:

John Gamble. As is standard under the Company's Insider Trading Policy, Mr. Gamble received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Gamble and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Gamble traveled to Utah with his wife on July 28 on non-Equifax business. On July 31, while in Utah, Mr. Gamble sent an email to the Legal Department requesting preclearance to sell 6,500 shares of Equifax stock (approximately 13.4% of his holdings at the time). Mr. Gamble's Equifax share grants had recently started to vest, and he had previously discussed with his financial adviser his goals to diversify his assets and to pay for an ongoing home renovation. Mr. Gamble's request to trade was approved via email on July 31, and the trade was executed on August 1.

Nine days after Mr. Gamble's trade, on August 10, during a management offsite meeting, Mr. Gamble first learned of the existence of a security incident at Equifax that was under investigation. Mr. Gamble received a more detailed briefing the following week, on August 17, and received additional details of the incident on August 22, during a Senior Leadership Team meeting.

[3] On August 15, 2017, the Equifax Legal Department imposed a trading blackout on all company personnel identified as aware of the breach as of that date. The Special Committee used the recipient list for the August 15 blackout notice to isolate the initial population of Equifax employees whose documents and communications should be reviewed. To the extent additional individuals were identified as potentially knowledgeable about the breach investigation during the Committee's review, their emails and texts were subject the same process, and those persons were interviewed.

The Special Committee concluded that Mr. Gamble did not have any knowledge of the security incident when he sought preclearance to trade on July 31 or when he executed his cleared trades on August 1. The Special Committee further concluded that Mr. Gamble fully complied with Company policy and did not engage in insider trading.

Trey Loughran: As is standard under the Company's Insider Trading Policy, Mr. Loughran received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Loughran and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Loughran sent an email to the Legal Department requesting preclearance to sell Equifax securities on July 28, 2017, one day before suspicious activity on the network was identified. On July 31, in response to a request from the Legal Department for greater specificity regarding the number and type of shares he wanted to sell, Mr. Loughran clarified that his request was to sell 4,000 shares (approximately 9.4% of his holdings at the time). Mr. Loughran's request for preclearance was approved on July 31, and the sale occurred on August 1. Mr. Loughran's sale of Equifax securities was consistent with previous sales he had made and was part of an effort to diversify his holdings.

Mr. Loughran first learned, at a general level, that a security issue was being investigated in a series of texts, emails, and phone calls he exchanged with members of the Equifax Legal Department on August 13 and 15. Mr. Loughran learned details of the breach on August 22, when he attended the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Loughran did not have any knowledge of the security incident when he sought preclearance to trade on July 28 or when he executed his cleared trades on August 1. The Special Committee further concluded that Mr. Loughran fully complied with Company policy and did not engage in insider trading.

Rudy Ploder: As is standard under the Company's Insider Trading Policy, Mr. Ploder received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Ploder and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Ploder sent an email to the Legal Department requesting preclearance to sell Equifax securities on August 1. Preclearance was granted that same day, and his trade executed on August 2. Mr. Ploder sold 1,719 shares (approximately 3.8% of his holdings at the time). Mr. Ploder's trade was motivated by, among other things, a need to meet costs associated with a business-related move to St. Louis and was consistent with his previous sales of Equifax shares.

Mr. Ploder learned of the security incident on August 22, 2017, when he participated in the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Ploder did not have any knowledge of the security incident when he sought preclearance to trade on August 1 or when he executed his cleared trades on August 2. The Special Committee further concluded that Mr. Ploder fully complied with Company policy and did not engage in insider trading.

Douglas Brandberg: As is standard under the Company's Insider Trading Policy, Mr. Brandberg received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Brandberg and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Brandberg sent an email to the Legal Department requesting preclearance to sell Equifax securities on August 1, 2017. Preclearance was granted on August 1, and his trade was executed on August 2. Mr. Brandberg sold 1,724 shares. Mr. Brandberg's sale of Equifax securities was consistent with his previous practice of selling shares as they vested; his sale was driven by family expenses.

Mr. Brandberg first learned that a security issue was being investigated on approximately August 14, and learned details of the security incident on August 22, when he attended the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Brandberg did not have any knowledge of the security incident when he sought preclearance to trade on August 1 or when he executed his cleared trades on August 2. The Special Committee further concluded that Mr. Brandberg fully complied with Company policy and did not engage in insider trading.

The Application of the Insider Trading Policy. Messrs. Gamble, Loughran, Ploder, and Brandberg each sought and received clearance from the appropriate Legal Department personnel prior to trading. Based on its review, the Committee has concluded that neither Equifax's Chief Legal Officer nor his designated preclearance officer had reason to believe that Messrs. Gamble, Loughran, Ploder, or Brandberg had knowledge of the security incident's existence as of the date of their preclearance requests or the date of their trades. Accordingly, the Special Committee has concluded that the preclearance authorization obtained by Messrs. Gamble, Loughran, Ploder, and Brandberg was within the authority permitted under the policy.

* * *

The Special Committee continues to review the cybersecurity incident, the Company's response to it, and all relevant policies and practices.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO PAULINE DO REGO BARROS, JR.

Question 1. On October 6, Equifax advised the Committee that it would send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. It also advised that it would mail written notices to all of the additional potentially impacted U.S. consumers—about 2.5 million—identified since the September 7 announcement. Please provide an update on the status of these notices, including what challenges Equifax has faced in attempting to comply with 52 separate data breach notification laws.

Answer. Equifax has completed mailing written notices to the three populations identified above. While the 52 separate data breach notification laws generally require notice to be sent to residents when a consumer's personal information is acquired in an unauthorized manner that compromises the security or confidentiality of that information, statutes vary with regard to several aspects of the breach notification requirements.

Generally, the most significant differences to reconcile include the threshold for issuing a substitute notice versus a direct notice, the required timing and content of the notification, regulator notices, and the definition of personally identifiable information ("PII").

While most states have the same general content requirements, some states have specific content requirements that typically require separate form notification letters in order to comply. As a result, the information consumers receive about a multistate incident may differ depending on where they reside and the requirements of their states. For example, California requires specific titles and headings, Massachusetts notifications cannot include information about the nature of the breach or the number of affected individuals, and Maryland and North Carolina require that state-specific Attorney General contact information be included in notices to their residents.

Notable variances in state breach notification statutes ultimately result in varying levels of information being provided to consumers and regulators depending on their state's specific requirements.

Question 2. Does Equifax support the enactment of a single Federal breach notification standard? If so, what form should it take?

Answer. 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:

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 have the same general content requirements and allow for a breached entity to provide a "standard" letter to a majority of impacted consumers that includes the date of the breach; a general description of the incident; the type of PII impacted; contact information for the breached entity; contact information for the consumer reporting agencies, the Federal Trade Commission and Attorneys General; steps taken to prevent a further breach; and advice to consumers regarding protecting against identity theft. Some states, however, have state-specific requirements that 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.

Regulator Notices & Enforcement: Some states require notice be provided to the state's Attorney General or other state regulators. 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.

Other provisions to consider when evaluating a Federal breach notification standard should include whether PII is "acquired" versus "accessed," whether 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."

Question 3. On October 6, Equifax advised the Committee that it is in the process of contacting U.S. state and Federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries. Please provide an update on the status of Equifax's efforts to contact U.S. state and Federal regulators regarding the breach.

Answer. Equifax notified the Federal Bureau of Investigation ("FBI") about the incident in question on August 2, 2017. Equifax notified the Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB") via phone calls on September 7, 2017, at approximately the same time Equifax published its official press release announcing the cybersecurity incident. In addition, Equifax provided written notifications to 52 state attorneys general on September 7, 2017. Upon the completion of the forensic investigation, Equifax also provided supplemental notifications to those 52 state attorneys general on October 12, 2017. We continue to cooperate with these regulators and law enforcement agencies, among others, in connection with the cybersecurity incident.

Question 4. At the time of the data breach, was Equifax in compliance with the FTC Safeguards Rule? If so, do you believe the fact that the data breach occurred signals that the rule should be strengthened?

Answer. Data security and integrity are of paramount importance to Equifax. Equifax has a formalized security program supported by administrative, technical, and physical safeguards focused on the protection of consumer data. Equifax has a security team in place that is responsible for the coordination and execution of the Company's information security program. The security team reports to Equifax's Chief Security Officer, who reports directly to Equifax's CEO, and operates using defined plans and procedures for responding to security incidents, which are revised on a regular basis. Security incidents are classified according to severity and escalated to management personnel as appropriate. The security team includes dedicated incident response managers and a Cyber Threat Center, which is staffed by security professionals and uses technological capabilities to monitor the Company's network. Equifax has physical safeguards in place to secure its data centers. The data security incident that Equifax disclosed on September 7, 2017, does not by itself suggest that the Safeguards Rule needs revision. Equifax will be better informed to make regulatory and legislative observations after the internal and external reviews of the incident have been completed.

Question 5. What specific steps has Equifax taken to comply with the Safeguards Rule since it discovered the data breach?

Answer. Equifax is conducting a root cause investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation.

Moreover, Equifax has already made important improvements to its data security infrastructure. It is further hardening its networks, changing its procedures to require "closed loop" confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on September 25, 2017. Equifax has also engaged PwC to help identify and implement a security program transformation, including tactical immediate changes, strategic remediation, and operational improvement initiatives that will allow the Company to strengthen its long-term data protection and cybersecurity posture.

Question 6. Does Equifax have any evidence showing that consumers have experienced identity theft or other harm as a result of the data breach? If so, please provide this evidence.

Answer. Equifax has not seen evidence that consumers have experienced identity theft or other financial harm as a result of the cybersecurity incident.

Question 7. Has Equifax identified any of the hackers or other persons or entities that obtained consumer information from the company in connection with the data breach?

Answer. Equifax is conducting an internal investigation into this incident and continues to work closely with the FBI in the FBI's investigation into this matter. At this time, Equifax is not aware that the perpetrators have been identified.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEAN HELLER TO PAULINE DO REGO BARROS, JR.

Question. Protecting data isn't just about the Internet—it's also about the physical security of data. In my home state of Nevada, we have the only Tier 5 rated data centers in the world. The best security and reliability you can get from a data center. What standards are you following to ensure that the data you manage is physically secure?

Answer. All Equifax facilities, including owned and operated data centers, are governed by the *Equifax Corporate Security Policy* and the *Equifax Physical Security Tier Standard.* Under the company's standard, Equifax data centers and data storage facilities are classified as "Tier 1—Critical Operations Facilities" and have the most stringent physical security requirements, including among others:

Security Intrusion Detection Systems and 24X7 Monitoring;

Man Traps;

Electronic access control systems;

Minimum two-factor authentication;

Formal access provisioning including formal visitor logs;

Cameras monitoring access points; and

Security guards.

In addition, Equifax performs annual Physical Security Surveys of data centers, which include assessments of the effectiveness and completeness of the controls in place based on identified risks to the data center and the requirements of the *Equifax Physical Security Tier Standard.* Equifax also performs preventative maintenance and testing of all electronic physical controls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO PAULINO DO REGO BARROS, JR.

Question 1. Under Florida state law, breached companies must notify affected consumers of a breach within 30 days. They can delay notification if they receive explicit permission from law enforcement. Was Equifax in compliance with Florida state law? Did the company receive permission from law enforcement to delay notification?

Answer. The Company worked diligently with Mandiant to conduct a detailed forensic analysis over the course of several weeks in order to determine what information was accessed and identify potentially impacted consumers in order to provide notification and an appropriate public disclosure of the incident. As soon as the company understood the potentially impacted population, it provided notification pursuant to all state data breach notification laws and rolled out a comprehensive support package to consumers on September 7, 2017.

Question 2. Do you agree that we need Federal legislation that sets up a robust breach notification requirement that sufficiently protects consumers, provides the Federal Trade Commission (FTC) with the authority to promulgate data security standards, and provides for strong Federal and state enforcement authority?

Answer. 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."

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RICHARD BLUMENTHAL TO PAULINO DO REGO BARROS, JR.

Question 1. Does any Federal agency currently have any kind of authority to examine Equifax's records and data security procedures?

Answer. Equifax is subject to continuous examination by the CFPB, as well the possibility of enforcement actions by the FTC and CFPB.

Question 2. Would you support efforts to protect the public's personal and private information by giving the FTC supervisory authority over non-bank financial institutions, such as credit reporting agencies?

Answer. Equifax supports efforts to protect the public's personal and private information, and is happy to engage with Congress about the specific details of any proposed legislation that would help achieve that goal.

Question 3. What is the difference between a credit lock and a credit freeze?

Answer. At the most basic level, the lock and freeze do the same thing: they prevent creditors and other lenders from accessing your Equifax credit report, including criminals trying to open unauthorized new accounts. Unless a consumer gives permission or takes an action, such as removing, unlocking or lifting the freeze or lock, a lender or other creditor cannot access the consumer's Equifax credit report with a security freeze or a credit file lock in place.

Security freezes (also known as credit freezes) were created in the early 2000s, are subject to regulation by each state, and use a PIN based system for identity authentication. Credit file locks were created more recently, are mobile-enabled, and use modern identity authentication techniques, such as username and passwords and one time passcodes for better user experience. The lock is a reliable, safe, and simple option for consumers to lock and unlock their credit file from their own personal device.

Detailed directions for freezing or locking an Equifax credit file are set forth on the company's website. The directions are paraphrased below:

> *Lock*—To lock your Equifax credit file, enroll in TrustedID Premier. This credit lock and monitoring service is free for one year to all consumers who enroll by

January 31, 2018. Once you have finalized your activation in TrustedID Premier, visit *www.trustedid.com,* login and simply click the lock button. There are some exceptions where a lock may be delayed or may not be possible. Once you have finalized your activation in TrustedID Premier, visit *www.trustedid.com,* login, and simply click the lock button.

To unlock an Equifax credit file, once you have finalized your activation in TrustedID Premier, visit *www.trustedid.com,* log in and simply click the unlock button.

Freeze—An Equifax security freeze can be placed by mail, phone, or online. Equifax has waived the fee to add, lift, or permanently remove a security freeze through January 31, 2018. Any freeze activities after January 31, 2018 may be subject to the fees provided by your state of residence. The easiest and fastest way to freeze your Equifax credit file is by using Equifax's online process found at the following link: *www.freeze.equifax.com.* If you choose, you may also request a security freeze by calling Equifax's automated line at 1–800–685–1111. NY residents please call 1–800–349–9960. You may also submit your request in writing to:

Equifax Security Freeze
P.O. Box 105788 Atlanta, Georgia 30348

When you freeze your Equifax credit file, you will receive a 10-digit randomly generated PIN from Equifax that you will need to save and have available should you choose to temporarily lift or permanently remove the freeze in the future.

Question 4. Brian Krebs, the founder of cybersecurity website *KrebsOn Security.com* has written that some credit lock services could allow for access to consumers' credit files that a freeze might not. What is your response to that concern?

Answer. Locking an Equifax credit file will prevent access to a consumer's Equifax credit file by certain third parties. Locking the Equifax credit file will not prevent access to the consumer's credit file maintained by any other credit reporting agency. Entities that may still have access to a consumer's locked Equifax credit file include companies like Equifax Global Consumer Solutions, which provide consumers with access to their credit report or credit score, or monitor the consumer's credit file; federal, state, and local government agencies; companies reviewing a consumer's application for employment; companies that have a current account or relationship with the consumer, and collection agencies acting on behalf of those whom a consumer owes; for fraud prevention and detection purposes; and companies that make pre-approved offers of credit or insurance to the consumer. Consumers can opt out of pre-approved offers at *www.optoutprescreen.com.*

Similarly, under state freeze laws certain third parties, like those mentioned above, may continue to have access to a frozen Equifax credit file.

Question 5. Can you commit that users of the new credit lock program, or any other program your company intends to offer to consumers to remedy their credit, will not be subject to mandatory arbitration clauses?

Answer. Equifax is not currently offering any subscription services to consumers for purchase. Equifax will not include an arbitration clause in connection with the forthcoming credit lock service that will be available in January 2018.

Question 6. Do you plan to target advertisements to users of this new credit lock program, or collect and sell their data?

Answer. Equifax intends to empower consumers with control over their Equifax credit file through the free lock service available at the end of January 2018. At this time, Equifax does not plan to include advertisements or sell the consumer's information to any third party. Equifax currently intends to use the information provided by the consumer to authenticate the consumer, maintain the consumer's Lock & Alert account, and educate the consumer about Equifax products and services.

Question 7. Why not create a service allowing users to easily *freeze* and temporarily unfreeze their credit—instead of 'lock' and 'unlock?

Answer. Please see response to question #3 (Blumenthal). Security freezes are free on Equifax credit reports through January 31, 2018.

Question 8. Are you collaborating with the other credit reporting agencies to develop a tool so consumers can easily freeze and unfreeze their credit across all agencies? If not, can you commit to doing so?

Answer. Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges we all face.

Question 9. Do you agree that users affected by the Equifax breach were harmed—even if they never ultimately become victims of identity theft of their data is not accessed?

Answer. Equifax believes that the best way for consumers to protect themselves and prevent any harm from occurring as a result of the incident is to enroll in TrustedID Premier and utilize the free lock service beginning in January.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO PAULINO DO REGO BARROS, JR.

Question 1. Please describe how Equifax informed Federal agencies, including the Department of Defense, the Department of Veterans Affairs, and the Consumer Financial Protection Bureau, that the private data of servicemembers and Veterans was potentially compromised. Please include the specific dates that Equifax notified each agency, copies of the notifications that were provided, and any advice and guidance Equifax provided on how best to protect Veterans and Servicemembers.

Answer. Equifax is committed to helping military service members. The company has been in direct communication with the Department of Defense (as of November 1, 2017) and CFPB's Office of Servicemember Affairs (as of October 24, 2017), and is working on efforts to inform servicemembers, including those impacted by the cybersecurity incident, regarding the incident and the various options available to them, such as the free TrustedID Premier service, security freezes, and active duty alerts, as well as other relevant information.

In addition, in response to the cybersecurity incident, Equifax developed a robust package of remedial protections for each and every American consumer—not just those affected by the breach—to protect their credit information. The relief package includes (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft, and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all Americans, including Veterans and servicemembers.

Question 2. Please share in detail the specific actions Equifax will take to ensure every Veteran and servicemember affected by this data breach will not have to worry about missing their disability check or becoming a victim of credit fraud.

Answer. In response to the cybersecurity incident, Equifax developed a robust package of remedial protections for each and every American consumer—not just those affected by the breach—to protect their credit information. The relief package includes (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft, and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all Americans, including Veterans and servicemembers.

Equifax has also taken steps to empower consumers to control access to their personal credit data moving forward. The Company announced a new credit lock service that will be available by January 31, 2018, that will allow consumers to control their own credit data, by allowing them to lock and unlock their credit files at will, for free, for life.

Finally, in addition to the services described above, security freezes, fraud alerts, and active duty alerts are available to help protect against credit fraud.

Question 3. If Equifax is unwilling to provide a guarantee of lifetime protections and credit freezes to servicemembers and Veterans, please explain why that is the case. Please include in your explanation any cost estimate(s) that Equifax produced or purchased projecting the cost of providing lifetime protection for Veterans, servicemembers, and any other class of American consumers for which Equifax obtained such cost estimates.

Answer. Equifax is committed to supporting and protecting our servicemembers and Veterans.

With respect to credit freezes, please note that in March 2017, the Consumer Data Industry Association announced that the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion) will begin offering free credit file security freezes for eligible members of the United States Armed Forces beginning in the first half of 2018. Under these new guidelines, active duty servicemembers will be able to place, lift, and remove a security freeze on their credit files at no charge, regardless of whether they have been the victim of identity theft or not.

Additionally, Equifax has announced a new service that will be available by January 31, 2018, that will allow consumers to control their own credit data, by allowing them to lock and unlock their credit files at will, for free, for life.

Finally, Equifax would gladly participate in discussions regarding recently proposed legislation and other Congressional proposals focused on protecting our servicemembers and Veterans.

Question 4. As of April 1, 2017, more than 1,500 credit fraud complaints had been filed by active duty servicemembers with the Consumer Financial Protection Bureau. With news of the breach at Equifax, that number is likely to increase exponentially over the coming year. According to the Fair Credit Reporting Act, servicemembers are protected by statute with an Active Duty Alert. Please share how often Equifax provides Active Duty Alerts for servicemembers and describe the process they must go through to place an Active Duty Alert on their information.

Answer. Any active duty member of the military may request an active duty alert for their Equifax credit file by using Equifax's online service, phone, fax, or U.S. mail. All active duty servicemembers can place an active duty alert either themselves or via a power of attorney.

By placing an active duty alert, (1) an alert will be included on the servicemember's credit report, which notifies creditors that they should take extra precaution to confirm the servicemember's identity before extending credit in his or her name, (2) the servicemember's name is removed from preapproved firm offers of credit or insurance (prescreening) for 2 years, and (3) information regarding the active duty alert is referred to all three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion), so the servicemember need only contact one and it will be activated on all three. Unless a shorter period of time is specified, the active duty alert lasts 12 months.

For more information regarding the number of active duty alerts placed in 2016 and 2017, please see the response to the question below.

Question 5. How many Active Duty Alerts for servicemembers did Equifax provide in calendar years 2016 and 2017?

Answer. During calendar year 2016, Equifax placed approximately 41,900 active duty alerts for servicemembers. During calendar year 2017, Equifax has placed approximately 86,200 active duty alerts for servicemembers.

Question 6. Will Equifax extend this alert to Reservists, National Guard Soldiers and Airmen, and Veterans by December 31, 2017? If not, please explain why.

Answer. Equifax respectfully submits that, as set forth in Section 605A(c) of the Fair Credit Reporting Act ("FCRA"), an active duty alert applies to active duty military consumers and must be directly requested by the active duty military consumer, or an individual acting on behalf of or as a personal representative of the active duty military consumer. However, even though an active duty alert applies only to active duty servicemembers, under the FCRA, Reservists, National Guard Soldiers and Airmen, and Veterans who are not on active duty can still place a fraud alert, which provides many of the same protections as an active duty alert, if they assert in good faith a suspicion that they have been or are about to become a victim of fraud or related crime, including identity theft.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO PAULINO DO REGO BARROS, JR.

Question 1. When can I expect a substantive response to my letter dated September 2017 regarding Equifax's position on mandatory pre-dispute arbitration clauses and S.J. 47, Senate legislation seeking to nullify the Consumer Financial Protection Bureau's rule limiting use of such clauses?

Answer. Equifax is not currently offering any subscription services to consumers for purchase. Equifax will not include an arbitration clause in connection with the forthcoming credit lock application that will be available in January 2018.

Question 2. Outside of the data (Social Security numbers, addresses, birth dates, driver's license numbers and credit card information) listed in your testimony in Committee, what other specific data does Equifax collect on consumers?

Answer. Equifax works with a wide range of data furnishers, vendors and with consumers directly to collect PII about consumers such as their names, tax identification numbers, e-mail addresses, phone numbers, IP addresses, and device identifiers. Equifax also works with data furnishers, partners, and vendors from many industries to gather information such as credit payment history, telecommunications and utilities payment history, employment and income history, public courthouse records, direct-measured deposits and investments, demographics, property detail and valuations, commercial payment history and profiles, education history, government sanctions lists, and auto-related information from sources such as motor vehicle registrations.

Question 3. Can you confirm what specific "digital targeting segments" of consumers that Equifax's IXI Service provides?

Answer. Equifax's IXI Service has over 400 "digital targeting segments" that are available on the market for use with delivering advertising to audiences in a digital environment.

Question 4. Is it true that among Equifax IXI's "digital targeting segments" are consumers who may need a "sub-prime credit card," a "revolver" (someone with a high balance and will have to accrue interest charges), a "likely student loan target," and "active debit card users?"

Answer. Yes.

Question 5. Do you support offering consumers the opportunity to view all the information held on them that is not displayed on credit reports?

Answer. When a consumer receives a copy of his or her credit report from Equifax Information Services LLC ("EIS"), the consumer receives all information EIS has on that consumer.

Question 6. Do you support offering consumers the opportunity to delete parts of their data?

Answer. Equifax will not offer consumers the opportunity to delete their personally identifiable information or remove accurate information on a credit report, except as required by law under the FCRA, 15 U.S.C § 1681 et seq., or applicable state laws.

As stated in the FCRA, "the banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system." 15 U.S.C § 1681, Sec. 602(a)(1). The law further states that the purpose of FCRA is "to require consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of [the FCRA]." *Id.* § 1681, Sec. 602(b).

Offering consumers the "opportunity to delete their data from Equifax's systems" would directly contradict the Federal obligation placed on consumer reporting agencies ("CRAs") to ensure that credit reports are accurate. Should a consumer delete accurate data from Equifax, or from any of the other CRAs, it would result in the creation of inaccurate credit reports which "directly impair the efficiency of the banking system," as noted above by the FCRA. It could also result in consumers potentially being considered "unbanked" by a lender, therefore unfairly hindering their access to credit.

In the *General Principles for Credit Reporting,* The World Bank has further concluded:

> "Information quality is the basic building block of an effective credit reporting environment. Accuracy of data implies that such data is free of error, truthful, complete and up to date. Inaccurate data may lead to numerous problems, including unjustified loan denials or higher borrowing costs." *General Principles for Credit Reporting,* The World Bank, September 2011, page 2.

In addition, The World Bank's International Committee on Credit Reporting also recently stated:

> "From a policy perspective, perhaps the most important role of credit reporting consists in addressing information asymmetries between creditors and borrowers in order to facilitate an efficient and cost effective credit risk assessment. Through this means, credit reporting can help achieve lower lending costs, which in competitive markets are passed on to borrowers in the form of lower cost of capital. Moreover, it can enhance access to credit for individuals and firms. Credit reporting also contributes to financial stability. For example, services offered by Credit Reporting Service Providers (CRSPs) help improve the quality of loans made by banks and other lenders through the provision of tools used to evaluate credit risk more effectively and consistently, as well as for the active management of the loan portfolio. Credit reporting also serves to discipline debtor behavior as regards the timely repayment of their financial and certain other obligations, as a good credit history facilitates access to credit and can often obviate the need for debtors to put up tangible collateral for loans." *The Role of Credit Reporting in Supporting Financial Sector Regulation and Supervision,* International Committee on Credit Reporting, The World Bank, January 2016, page 5.

Accurate and complete data "facilitate[s] an efficient and cost effective credit risk assessment" and "contributes to financial stability." The opportunity for consumers to selectively delete accurate information from CRAs would directly prevent a critically important component of our financial system.

Under the FCRA, consumers have the right to receive a free, annual copy of their credit report and to review the accuracy of the information included on that report. In addition, consumers are entitled to a free report in the event of an adverse action, such as the denial of an application for credit, insurance, or employment, based on information in the report. Further, consumers are entitled to a free, annual copy of their credit report if they are unemployed and plan to look for a job within 60 days; if the consumer is on welfare; or if a report is inaccurate because of fraud, including identity theft.

Further, under the FCRA, CRAs, and furnishers of information provided to the CRA, are responsible for correcting inaccurate or incomplete information on a credit report, and must comply with established procedures outlined in the FCRA to enable consumers to dispute information on their credit file.

Equifax complies with the above obligations under the FCRA, which support the underlying goal of ensuring a system of "fair and accurate credit reporting" for the benefit of consumers, lenders and the entire financial system.

Question 7. Was the Chief Legal Counsel who approved of the stock sales also aware that the firm contemporaneously contacted the FBI and Mandiant?

Answer. The Equifax Legal Department approvals of the referenced stock sales were not made "contemporaneously" with the contacts with the FBI and Mandiant, as further explained below.

The Board of Directors of Equifax released a report by a Special Committee of the Board of Directors regarding the trading of Company securities by certain executives following the detection by Equifax cybersecurity personnel of suspicious activity in the Company's network and prior to public disclosure of the incident. A copy of the report by the Special Committee and accompanying press release was provided to the Committee on November 3, 2017. A copy of that report is also enclosed with this submission. The report concludes that two of the executives whose trades were reviewed received clearance from Legal Department personnel on July 31, 2017, and two other executives received Legal Department clearance on August 1, 2017.

Based on the early indications of suspicious activity, on August 2, 2017, (1) the Company's Senior Vice President, U.S. Legal—on behalf of Equifax—retained the cybersecurity group at the law firm of King & Spalding to guide the forensic investigation and provide legal and regulatory advice; (2) King & Spalding engaged the independent cybersecurity forensic firm, Mandiant, to aid in investigation of the suspicious activity; and (3) the Company contacted the FBI. It was not until later in August that the forensic investigation determined the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables. The Chief Legal Officer was not aware of these engagements or the contact of the FBI before they were made, but became aware of them after they occurred.

Question 8. Did the Chief Legal Counsel approve any contracts with Mandiant related to the July 29th "suspicious traffic?"

Answer. The Chief Legal Officer was not involved in reviewing or approving the agreement with Mandiant. The Company's Vice President Legal reviewed and approved the agreement.

Question 9. What dividends did Equifax pay out to shareholders following knowledge of the data breach?

Answer. Since the company's security team discovered the unauthorized access on July 29, the company declared (1) a quarterly dividend on August 4, 2017 of $0.39 per share, which was paid on September 15, 2017, and (2) a quarterly dividend on November 9, 2017 of $0.39 per share, which is payable on December 15, 2017. Decisions regarding the declaration and payment of dividends depend on the company's financial condition, earnings, prospects, current and future funding requirements, applicable law, and other relevant factors. The dividends paid in 2017 reflect consideration of these factors.

Question 10. Why did Equifax elect to pay out dividends to shareholders given knowledge of the company's tremendous legal exposure and the harm caused to consumers?

Answer. Decisions regarding the declaration and payment of dividends depend on the company's financial condition, earnings, prospects, current and future funding requirements, applicable law, and other relevant factors. The dividends paid in 2017 reflect consideration of these factors.

Question 11. Can you provide a list of every data breach or incursion Equifax has experienced since 2010?

Answer. Equifax does have a system for tracking data breaches and incidents. Equifax will provide a list responsive to this request as soon as possible.

Question 12. What resources is Equifax making available to ensure that community banks and credit unions are made whole as a result of this data breach?

Answer. Following the announcement of the cybersecurity incident, Equifax has met with and continues to work with community banks and credit unions to provide them information about the cybersecurity incident and to respond to specific questions raised. Equifax also made available communication materials (*i.e.,* FAQs) to the community banks and credit unions that provide information about the cybersecurity incident to their customers and members. Equifax continues to accommodate requests from community banks and credit unions to further discuss the cybersecurity incident.

Question 13. Can Equifax provide data on the number of active duty servicemembers and seniors impacted by the data breach, broken down by state?

Answer. Active duty status is not a data element that Equifax possesses. As a result, Equifax is unable to calculate the number of impacted active duty servicemembers. It is difficult to accurately assess the number of impacted seniors. The dates of birth included within the data associated with the cybersecurity incident consist of self-reported birth dates or not dates at all and as a result, the information may not be reliable for purposes of calculating the total number of seniors impacted by the incident. For example, some dates in the data do not appear to reflect accurate dates of birth (*e.g.,* 1/1/1111).

Question 14. Does Equifax take any actions to confirm or scrutinize the data breach protections of the companies and organizations that it sells and markets consumer information to?

Answer. Yes.

Question 15. Will you help Congress improve consumer protections by supporting legislation to institute a stronger regulatory framework for entities such as yourself to help ensure everyone responsible for protecting consumers have improved defenses in place?

Answer. Equifax supports efforts to protect the public's personal and private information, and is happy to engage with Congress about the specific details of any proposed legislation that would help achieve that goal.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEAN HELLER TO MARISSA MAYER

Question. Protecting data isn't just about the Internet—it's also about the physical security of data. In my home state of Nevada, we have the only Tier 5 rated data centers in the world. The best security and reliability you can get from a data center. In your experience as Former President and CEO of Yahoo!, what standards did you follow to ensure that the data managed by Yahoo! was physically secure?

Answer. Throughout my tenure as CEO, we took our obligations to our users and their security extremely seriously. Yahoo had in place multiple layers of sophisticated protection, including strict controls over the security of its data centers located throughout North America, South America, Europe, and Asia. Yahoo deployed strong, industry standard physical, technical, and procedural safeguards in accordance with relevant regulations to protect user data. Cross-company initiatives such as HTTPS end-to-end encryption helped to further strengthen the company's security defenses and protect its users.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO KAREN ZACHARIA

Question 1. Regarding the 2013 and 2014 breaches, Yahoo! has pointed out that the stolen information did not include social security numbers, clear text passwords, or other sensitive financial information. Nevertheless, the account information that was compromised did include information that could be used to access sensitive information. Consumers have been known to e-mail personal information, password reminders, as well as other sensitive details to themselves or others. And while Yahoo! took action around the time of its announcements to protect its user accounts, at least with respect to the 2013 breach, there was *a three-year window* during which these accounts were unprotected. Does Verizon have any evidence showing that consumers were exposed to higher risk based on information subsequently

accessed from user accounts using stolen credentials? If so, please provide this evidence.

Answer. Verizon has no evidence that the data elements taken by the intruders in the 2013 and 2014 data thefts—including names, e-mail addresses, telephone numbers, dates of birth, hashed passwords and encrypted or unencrypted security questions and answers—resulted in access and use of information in consumers' e-mail content to perpetrate identity theft or financial fraud. Yahoo has received complaints (*e.g.,* via Yahoo Customer Care and civil lawsuits arising from the 2013 and 2014 data thefts), some of which allege that harm has occurred as a result of the 2013 and 2014 data thefts. However, these claims have not been substantiated or causally connected to the data thefts. In addition, Yahoo's systems would trigger additional verification requirements, including a second login challenge, that would provide security for accounts beyond the users' hashed passwords (which were not taken in clear text in either incident). Yahoo also has taken additional steps to enhance user security, including the strengthening of internal controls and a forced password reset for users. Yahoo also has encouraged users to adopt key-based authentication in lieu of passwords.

Further, as the Department of Justice stated in a press release, one of four state sponsored hackers who was indicted for the criminal intrusions "exploited his access to Yahoo's network for his personal financial gain, by searching Yahoo user communications for credit card and gift card numbers. . . ." Dept. of Justice, Office of Public Affairs, U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of E-mail Accounts, March 15, 2017, at p. 1. We have no evidence, however, that the content of any of the user communications referenced in the press release were used to perpetrate identity theft or resulted in financial fraud.

Question 2. Does Verizon support the enactment of a single Federal breach notification standard? If so, what form should it take?

Answer. Yes, Verizon supports enactment of a Federal breach notification law that would set a national standard. This would provide consumers across the country with consistent notices and will lead to a greater understanding by consumers about why they are being notified and what actions might be appropriate for them to take. The following two elements are particularly important to include in a Federal breach notification law: (a) mandating notices in the appropriate circumstances, such as when there is a material risk of identity theft or financial fraud, thus avoiding over-notification which desensitizes consumers to the notices they receive; and (b) preempting the existing state patchwork framework that currently exists which leads to consumer confusion.

Response to Written Question Submitted by Hon. Bill Nelson to Karen Zacharia

Question. Do you agree that we need Federal legislation that sets up a robust breach notification requirement that sufficiently protects consumers, provides the Federal Trade Commission (FTC) with the authority to promulgate data security standards, and provides for strong Federal and state enforcement authority?

Answer. Verizon supports the enactment of a Federal data security and breach notification law that would set a national standard. Such a law would provide consumers across the country with consistent protections and notices. It will also lead to a greater understanding by consumers about why they are being notified and what actions might be appropriate for them to take. The following two elements are particularly important to include in a Federal breach notification law: (a) mandating notices in the appropriate circumstances, such as when there is a material risk of identity theft or financial fraud, thus avoiding over-notification which desensitizes consumers to the notices they receive; and (b) preempting the existing state patchwork framework that currently exists which leads to consumer confusion.

With regard to data security, whether it would be appropriate for the Federal Trade Commission to promulgate standards would depend on the structure of the data security provisions of a Federal law. With regard to enforcement authority, we believe that is a role most appropriate for the Federal Trade Commission. Whether state authorities should also have enforcement authority would depend on the structure and provisions of the law, such as available remedies.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO KAREN ZACHARIA

Question 1. What specific types of data does Yahoo and Verizon, respectively, collect on consumer? Please list each individual piece of consumer information both entities collect and maintain.

Answer. The *Verizon Privacy Policy* details the specific types of data Verizon collects. The full privacy policy is available at *http://www.verizon.com/about/privacy/full-privacy-policy.* A summary of certain relevant portions of the Verizon Privacy Policy is included below:

- Verizon collects information when consumers use our products, services and sites, including call records, websites visited, wireless location, application and feature usage, network and device data including battery life and apps on a consumer's device, product and device-specific information and identifiers, service options chosen, mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, TV and other video viewership, and other similar information.
- Verizon also collects information consumers provide such as name and contact information, images, voice recordings or voice prints, the reason for contacting us, driver's license number, Social Security Number and payment information.
- Verizon may monitor or record communications with customers or keep a record of these transactions.
- Verizon collects information about consumer's user identification, password and secret questions and answers when they establish an online account or register on our sites or apps.
- Verizon also obtains information from third parties, including credit information from outside credit reporting agencies related to consumers applying for service with us. Verizon also obtains information from outside companies such as those that collect consumer information including demographic and interest data.

The *Yahoo Privacy Policy* details the specific types of data Yahoo collects. The full privacy policy is available at *https://privacy.yahoo.com.* A summary of certain relevant portions of the Yahoo Privacy Policy is included below:

- Yahoo collects personal information when a user (i) registers with Yahoo; (ii) uses Yahoo products or services; (iii) visits Yahoo pages or the pages of certain Yahoo partners; and (iv) enters a promotion or sweepstakes.
- Upon registration, Yahoo asks for the user's name, e-mail address, birth date, gender, ZIP code, occupation, industry, and personal interests. For some products and services, such as certain services available on Yahoo Finance, Yahoo may also ask for a user's address and information about assets. Yahoo also stores the user's IP address in its registration databases at the time of registration.
- Yahoo collects information about user transactions with Yahoo and with some of Yahoo's business partners, including information about the user's use of products and services that Yahoo offers.
- Yahoo's automated systems analyze communications content, including incoming and outgoing user e-mails.
- As part of using any Internet based services, Yahoo automatically receives and records information from its users' computers and browsers, including user IP address, Yahoo cookie information, software and hardware attributes, and the page a user requests.
- Analytic tools such as Yahoo Analytics, Advertising Insights, and Flurry from Yahoo use web beacons, cookies, and similar technologies to collect data about visitors to Yahoo's sites and apps and its customers' sites and apps.
- Yahoo may obtain information from its partners and append it to its existing user information to provide more relevant content and advertising for users.
- In certain situations, Yahoo also collects location data. If a user provides permission, Yahoo may obtain pinpointed physical location information from technologies like GPS, Wi-Fi, or cell tower proximity. Yahoo also may collect data on locations that a user searched for in certain properties (such as Search and Maps) as well as other location data provided by the user (such as postal code) to Yahoo.

Oath is currently reviewing this Privacy Policy to align Yahoo and AOL policies and it may make changes in the future.

Question 2. When consumers delete their account or Yahoo, or Verizon deactivates their accounts, do companies continue to store their user data?

Answer. Verizon's policy is to maintain information about former subscribers to our telecommunications services for as long as it is reasonably necessary for business, operational, tax, or legal purposes. This information may include name and contact information, payment information, service usage information such as call records, and service options they chose among other things.

Yahoo's website provides account details, including information about account deletion, available at *https://policies.yahoo.com/us/en/yahoo/privacy/topics/datastorage/index.htm.* Following a user's request for account deletion, a hold period is activated—this hold period varies by jurisdiction and is in place, among other reasons, to enable users to reactivate their account if they initiated an account deletion in error. Following the hold period, Yahoo will process the user's account deletion request. This will result in data associated with the user's registered account to be either deleted or anonymized. There may be exceptions, however, including when there is a legal hold obligation for litigation preservation or other limitations, including those technical in nature.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO TODD WILKINSON

Question. Do you agree that we need Federal legislation that sets up a robust breach notification requirement that sufficiently protects consumers, provides the Federal Trade Commission (FTC) with the authority to promulgate data security standards, and provides for strong Federal and state enforcement authority?

Answer. I do agree that a standardized breach notification requirement should be instituted. The breach notification must first establish a timeline for such a notification to consumers, but must also take in to consideration the timeline required by an organization to fully understand if a breach occurred. Every breach is different and detection needs to be verified before imposing a breach notification requirement on the affected business. Expanding the Federal Trade Commission's (FTC) ability to oversee these regulations and any subsequent enforcement actions will need to be decided upon by our congressional leadership. Regardless of who is promoting legislation, if the consumer notification process is to improve, it is critical that the legislation include meaningful enforcement regulations.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. RICHARD BLUMENTHAL TO TODD WILKINSON

Question. Should Credit Rating Agencies be adequately audited for cyber hygiene practices and compliance with the FTC's Safeguards Rule, which implements the Gramm-Leach-Bliley Act and provides data security requirements for non-bank financial institutions?

Answer. Yes, absolutely—and not just for financial institutions or credit rating agencies. Any organization that touches personally identifiable information (PII) should be subject to a minimum requirement of data security hygiene. There are several government and industry bodies (*e.g.,* NIST and SANS respectively) that provide regular recommendations for data security best practices. While it would be impossible to write legislation to keep up with the rapidly evolving threat landscape, it would be possible to refer to one of these current frameworks as a minimum standard. But putting a baseline in place will only be successful if there is sufficient oversight and meaningful enforcement of the regulations.

○

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.