

EXAMINING THE EQUIFAX DATA BREACH

HEARING BEFORE THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION

OCTOBER 5, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115-46



U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2018

30-242 PDF

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina,
Vice Chairman

PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking
Member*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

C O N T E N T S

| | |
|-----------------------|------|
| | Page |
| Hearing held on: | |
| October 5, 2017 | 1 |
| Appendix: | |
| October 5, 2017 | 63 |

WITNESSES

THURSDAY, OCTOBER 5, 2017

| | |
|--|---|
| Smith, Richard F., Adviser to the Interim Chief Executive Officer and Former Chairman and Chief Executive Officer, Equifax | 5 |
|--|---|

APPENDIX

| | |
|------------------------|----|
| Prepared statements: | |
| Smith, Richard F. | 64 |

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

| | |
|---|-----|
| Waters, Hon. Maxine: | |
| Letter to Chairman Hensarling | 85 |
| Ellison, Hon. Keith: | |
| Letter from Consumers Union | 72 |
| Maloney, Hon. Carolyn: | |
| Letter to TransUnion and Experian | 80 |
| Letter from Experian | 82 |
| Messer, Hon. Luke: | |
| Equifax Privacy Notice | 84 |
| Smith, Richard F.: | |
| Written responses to questions for the record submitted by Ranking Member Waters | 87 |
| Written responses to questions for the record submitted by Representative Ellison | 94 |
| Written responses to questions for the record submitted by Representative Heck | 95 |
| Written responses to questions for the record submitted by Representative Meeks | 99 |
| Written responses to questions for the record submitted by Representative Sinema | 100 |
| Report of the Special Committee of the Board of Directors of Equifax, Inc. | 101 |

EXAMINING THE EQUIFAX DATA BREACH

Thursday, October 5, 2017

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The committee met, pursuant to notice, at 9:19 a.m., in room 2128, Rayburn House Office Building, Hon. Jeb Hensarling [chairman of the committee] presiding.

Present: Representatives Hensarling, Royce, Lucas, Pearce, Posey, Luetkemeyer, Huizenga, Duffy, Stivers, Hultgren, Ross, Pittenger, Wagner, Barr, Rothfus, Messer, Tipton, Williams, Poliquin, Love, Hill, Emmer, Zeldin, Trott, Loudermilk, Mooney, MacArthur, Davidson, Budd, Kustoff, Tenney, Hollingsworth, Waters, Maloney, Velazquez, Sherman, Meeks, Capuano, Clay, Lynch, Scott, Cleaver, Ellison, Perlmutter, Himes, Foster, Kildee, Delaney, Sinema, Beatty, Heck, Vargas, Gottheimer, and Gonzalez.

Chairman HENSARLING. The committee will come to order.

Without objection, the Chair is authorized to declare a recess of the committee at any time, and all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record.

The hearing is entitled “Examining the Equifax Data Breach.”

I now recognize myself for 3–1/2 minutes to give an opening statement.

On September 7, Equifax announced what it called a, quote, “cybersecurity incident” at its business that potentially affects 145 million U.S. consumers—nearly half of all Americans. In other words, if you are hearing my voice, you are either the victim of the breach or you know someone who is. That is how massive this breach was.

The criminals got basically everything they need to steal your identity, open credit card accounts in your name, and cause you untold frustration and financial calamity. This may be the most harmful failure to protect private consumer information the world has ever seen.

The company’s response to this breach has left much to be desired. For weeks, Equifax failed to disclose the breach to consumers and its shareholders. It provided confusing information about whether people were victims of the breach or not.

And, beyond belief, senior executives sold their Equifax shares after the company knew of the breach and before the company disclosed the breach. I trust the Justice Department and Securities Exchange Commission (SEC) will get to the bottom of this.

Clearly, action by the Federal Trade Commission, the Consumer Financial Protection Bureau, and potentially other regulators is required. Congress must ensure that Federal law enforcement and Federal regulators do their jobs so justice can be served and victims are made whole.

We must thoroughly examine if our agencies in statutes like Gramm-Leach-Bliley, the Fair Credit Reporting Act, and UDAAAP are up to the job.

In this era, big data, large-scale security breaches unfortunately are becoming all too common. By the increasing frequency and sophistication of cyber attacks, this clearly demands heightened vigilance and enhanced efforts to safeguard consumers.

Protecting consumers obviously starts with requiring effective measures to prevent data breaches in the first place. Given the Federal Government's own poor track record when it comes to protecting personal information witness the SEC and the Office of Personnel Management (OPM) hacks as two recent examples.

We must be cautious about attempts to never let a good crisis go to waste and impose a Washington-forced technology solution that may be antiquated as soon as it is imposed. However, I do believe that we need to ensure we have a consistent national standard for both data security and breach notification in order to better protect our consumers, hold companies accountable, and assure that this affair does not repeat itself.

Our committee passed such legislation nearly 2 years ago, the bipartisan Data Security Act. The need to revisit that legislation and, where necessary, improve upon it should be obvious to all. The status quo is clearly failing consumers and leaving them extremely vulnerable.

So I look forward to working with members of both sides of the aisle and working with the Administration to ensure that Americans across the country will be protected and will no longer have to lose sleep over the kind of breaches that we are discussing today.

I yield back the balance of my time.

I now recognize the Ranking Member of the Committee, the gentlelady from California, for 3 minutes.

Ms. WATERS. Thank you, Mr. Chairman.

The massive breach at Equifax and the company's subsequent failures are a lapse on a scale we have never seen before. Equifax's failure to safeguard consumer data is all the more egregious because the impacted customers never chose to do business with Equifax.

And because of the broken business models of our country's credit reporting agencies, these consumers can't end their relationship with Equifax. They can't shop around for a better deal. They are literally stuck with this company.

So I am very interested in what Equifax will do moving forward to provide full redress for all of those who have been harmed. I am also interested in why Equifax has sent this committee a witness today without the authority to commit Equifax to future action.

The members of this committee need to hear not just about what has happened but also about what Equifax plans to do moving for-

ward. I already know that this hearing won't answer all of the questions, and I and other members would like to know more.

This is why committee Democrats are requesting a minority day hearing to get more answers to the questions surrounding not only this breach but also its impact on consumers and solutions for consumers moving forward.

For example, I, for one, would like to make sure that credit reporting agencies do not inappropriately profit off of this incident by exploiting consumers' legitimate fears. Now is not the time to focus on how to sell consumers more products. Now is the time to fix what has been broken.

But this breach and Equifax's woeful response are just the tip of the iceberg. The whole credit reporting system needs a complete overhaul. That is why I introduced H.R. 3755, the Comprehensive Consumer Credit Reporting Reform Act. This legislation would, among other things, shift the burden of removing credit report mistakes to credit reporting agencies and away from consumers.

And my bill would also shrink the importance of credit reports in our lives by limiting the use of credit reports in employment checks and limiting when CRAs can collect information on consumers. It is time to end the strangledhold that Equifax, TransUnion, and Experian have on our consumers' lives.

Mr. Chairman, I yield back.

Chairman HENSARLING. The gentlelady yields back.

The Chair now recognizes the gentleman from Missouri, Mr. Luetkemeyer, the Chairman from our Financial Institutions Subcommittee for 1-1/2 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

Mr. Smith, I know you have sat before several committees this week, and I trust you have heard the anger from Congress and the American people. This is not just incompetence on the part of you and your company but also negligence and disregard for the law and for consumers.

There is a failure on the part of you, your board, and your senior management, and your failures have impacted more than one-third of the American people. What is most egregious to me is that the American people's data had potentially been compromised, had to wait more than a month to find out about it.

The American public deserves better. They deserve prompt notification so they can safeguard their identity. They deserve a system that effectively and efficiently notifies them, not one that has slowed down because of turf wars, regulatory complex, or fear of litigation.

I believe it is now time to move forward, and we need to find solutions to this problem. I hope that if one good thing comes from this yet another major data breach, it is that the American consumers can finally get a system that works for them.

I Chair the Financial Institutions Subcommittee that is going to have oversight over this data breach and a security informational-type of bill, and I can assure you we are going to try and look very thoroughly at this incident as others drum up some ways to protect the American consumers.

Mr. Chairman, with that, I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Missouri, Mr. Clay, the Ranking Member of the Financial Institutions Subcommittee for 1 minute. Apparently he is not here.

We then will go to the gentleman from Michigan, who also appears not to be here.

The gentleman from Minnesota, Mr. Ellison, is recognized for 1 minute.

Mr. ELLISON. I would like to thank the Chair and Ranking Member for this important hearing.

A lot has been said about the Equifax breach and a lot of the same things will be repeated today, but there are a few things that I think we have to bear in mind: One is that Equifax and two other big players in this industry of credit reporting dominate basically the whole field.

As members of this committee know, I have been quite concerned about market concentration. I believe Equifax is just too big. It needs to be reduced in size. We need to increase competition and we need—and if Equifax had to worry about a real competitor, I believe they would be better at safeguarding the data of consumers.

It is the fact that markets have concentrated it so high that other than TransUnion and Experian, Equifax doesn't have to worry about much competition—that they can be lax with the data of people.

I look forward to the gentleman talking about some issues that I think are very important. I know that there has been some movement in the area of—well, I will leave that to you for the rest of the questioning.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentlelady from New York, Mrs. Maloney, Ranking Member of the Capital Markets Subcommittee for 1 minute.

Mrs. MALONEY. Mr. Smith, Equifax was not just a breach of security. It was not just a massive, huge database breach. It was a breach in the trust of the American people in your company.

We have the best markets in the world, and I believe that our markets run more on trust than it does on capital. So a breach of trust is something our markets cannot tolerate.

I join my colleagues in being committed to finding procedures going forward that this does not happen again, and that the law is enforced against those who breach and break the law.

Chairman HENSARLING. The time of the gentlelady has expired.

Today we will receive the testimony of Mr. Richard Smith, who is the former CEO and Chairman of Equifax and adviser to the interim CEO. Prior to September 26 of this year, Mr. Smith had been the Chairman and Chief Executive Officer at Equifax since 2005. Before joining Equifax, Mr. Smith held various management positions at General Electric where he worked for 22 years.

Without objection, the witness' written statement will be made part of the record.

Mr. Smith, you are now recognized for 5 minutes to give an oral presentation of your testimony. Thank you.

STATEMENT OF RICHARD F. SMITH

Mr. SMITH. Thank you. Thank you Chairman Hensarling, Ranking Member Waters, and the honorable Members of the committee. Thank you for allowing me to come before you today to testify. Again, I am Rick Smith, and for the past 12 years, I have had the honor of serving as Chairman and CEO of Equifax.

Over the past month or so, I have had the opportunity to talk to many American consumers and read their letters, those impacted and not impacted alike, and understand their anger and frustration that we have caused at Equifax.

This criminal attack on our data occurred on my watch, and I take full responsibility for that attack as the CEO. I want every American and everyone here to understand that I am deeply apologetic and sorry that this breach occurred; and that, I also want the American public to know that Equifax is committed to dedicate our energy and time going forward to making things right.

Americans have a right to know how this happened, and today I am prepared to testify about what I learned and what I did about this incident while CEO of the company, and also what I know about the incident as a result of being briefed by the company's ongoing investigation.

We now know that this criminal attack was made possible by a combination of a human error and a technological error. The human error involved the failure to apply a patch to a dispute portal in March 2017. The technological error involved a scanner that failed to detect the vulnerability on this particular portal that had not been patched. Both errors have since been addressed.

On July 29 and 30, the suspicious activity was detected. We followed our security incident response protocol at that time. The team immediately shut down the portal, and they began their internal security investigation.

On August 2, we hired top cybersecurity forensic and legal experts. We also notified the Federal Bureau of Investigation (FBI). At that time, we did not know the nature or the scope of the incident. It was not until late August that we concluded that we had experienced a major data breach.

Over the weeks leading up to September 7, our team continued working around the clock to prepare to make things right. We took four steps to protect consumers: First, determining when and how to notify the public, relying on the advice of our experts that we needed to have a plan in place as soon as we announced; No. 2, helping consumers by developing a website, staffing up massive call centers, and offering free services not only to those impacted but to all Americans; No. 3, preparing for increased cyber attacks, which we were advised are common after a company announces a breach; and finally, No. 4, continuing to coordinate with the FBI in their criminal investigation of the hackers while at the same time notifying Federal and State agencies.

In the rollout of our remediation program, mistakes were made for which I am, again, deeply apologetic. I regret the frustration that many Americans felt when our websites and our call centers were overwhelmed in the early weeks. It is no excuse, but it certainly did not help that two of our larger call centers were shut down due to Hurricane Irma.

Since then, however, the company has dramatically increased its capacity. And I can report to you today that we have had over 420 million U.S. consumers visit our websites and that our call times, our wait times at the call centers have been reduced substantially.

At my direction, the company offered a broad package of services to all Americans, all of them free, aimed at protecting the consumers. In addition, we developed a new service available on January 31 of 2018 that will give all consumers the power to control access to their credit data by allowing them to lock and unlock access to their data for free for life, putting the power to control access to credit data in the hands of the American consumer. I am looking forward to discussing in as much detail as you would like that service offering during my testimony.

As we have all painfully learned, data security is a national security problem. Putting consumers in control of their credit data is a first step toward a long-term solution to the problem of identity theft.

But no single company can solve a larger problem on its own. I believe we need a private–public partnership to evaluate how to best protect Americans’ personal data going forward, and I look forward to being a part of that dialog.

Chairman Hensarling, Ranking Member Waters, and honorable Members of the committee, thank you again for inviting me to speak today. I will close again by saying how sorry I am that this breach occurred on my watch.

On a personal note, I want to thank the many hardworking and dedicated employees that I worked with so tirelessly over the past 12 years. Equifax is a very good company with thousands of great people trying to do what is right every day. I know they will continue to work tirelessly as we have over the past few months to right the wrong.

Thank you.

[The prepared statement of Mr. Smith can be found on page 64 of the Appendix.]

Mr. SHERMAN. Mr. Chairman, point of order.

Chairman HENSARLING. The gentleman from California will state his point of order.

Mr. SHERMAN. I would request that the witness be sworn.

Chairman HENSARLING. It has not been the practice of the committee to swear in witnesses, as you know. The witness has to sign before coming here that the testimony will be truthful. That should be sufficient.

The Chair yields himself 5 minutes for questions.

Mr. Smith, I know this is your fourth appearance before Congress, but I think you know it speaks to the gravity of the situation, the number of our constituents which are impacted and, frankly, the number of committee jurisdiction lines that this crosses.

Since you have testified three other times, I will attempt to plow a little new ground. As you know, there is a lot of focus on—I guess to use your phrase—once the nature and the scope of the breach was realized, this still took approximately a month before people were notified of the breach.

Did someone in law enforcement ask Equifax to delay notification to the public?

Mr. SMITH. Mr. Chairman, as I mentioned in my written and oral comments, we were in communication routinely throughout the process with the FBI, but they did not necessarily dictate the flow of communication to the public.

Chairman HENSARLING. OK. Were there outside data security consultants that advised the company to delay notification for a month?

Mr. SMITH. Mr. Chairman, we worked very closely with Mandiant—that may ring a bell. Mandiant is viewed as, if not the leading, one of the leading cyber forensic firms in our country—and our outside counsel, global law firm King & Spalding. And, yes, they both, in tandem with our team, managed the flow of communication externally.

I would say, Mr. Chairman, one thing—

Chairman HENSARLING. I am sorry. Did they advise you to delay it for approximately 4 weeks?

Mr. SMITH. They guided us in our announcement on the 7th. The 4 weeks—Mr. Chairman, it wasn't until around the 24th that we really realized the size of the breach, and even that continued to develop from the 24th of August until the time we went public on the 7th.

And as you may have seen, the company came out, I think it was this Monday, with continued evidence on 2.5 million more consumers. So it was a very fluid process of understanding the scope, the size, and the nature of the breach.

Chairman HENSARLING. Mr. Smith, I am led to believe the Apache Struts CVE-20175638 vulnerability was first publicized in early March, at which point it was immediately categorized as a critical vulnerability by numerous cybersecurity authorities. What do you believe is a reasonable amount of time for a critical vulnerability patch to be pushed out and implemented on all affected applications?

Mr. SMITH. Yes. Our policy, our program at the time was within 48 hours and we did that. We were notified—

Chairman HENSARLING. I am sorry. You did do that?

Mr. SMITH. Yes.

Chairman HENSARLING. So what happened?

Mr. SMITH. So on the 8th of March we were notified, as you mentioned. On the 9th of March, following the standard protocol, the communication was disseminated to those who needed to know about the patch.

Two things happened, Mr. Chairman: One was a human error, an individual who was responsible for what we call the patching process did not ensure that there was communication and closed-loop communication to the person who needed to apply the patch. That was error number one.

Error number two was on the 15th of March, we used a technology called a scanning technology, which looks around the systems for vulnerabilities. That scanner, for some reason, did not detect the Apache vulnerability. So we had a human error, as I alluded to in my oral testimony, and a technological error, both resulting in the fact that it was not patched.

Chairman HENSARLING. Mr. Smith, once Equifax chose to notify the public—there are currently roughly 47-odd State breach notification laws, as you are well aware. So I know we have a patchwork. But under what breach notification regime did you notify the public?

Mr. SMITH. Well, Mr. Chairman, we were mindful of the State laws and trying to abide by all the State laws, while at the same time following the recommendation of Mandiant, making sure we had clear and accurate understanding of the breach. And as I mentioned earlier, that took weeks.

It was very difficult to retrace the footprints of these criminals, where they had been, what they had done. We had to recreate inquiries, we being Mandiant and the security team and our outside legal adviser. That took a long time.

Chairman HENSARLING. Mr. Smith, you are located in Georgia, correct? Was that a Georgia regime notification that you followed? You didn't follow the 47-odd State notification regimes, did you?

Mr. SMITH. Yes, sir, we are headquartered and domiciled in Atlanta, Georgia. My point was we were aware of and mindful of all State laws for breach notification while also making sure we had an accurate and clear understanding of what data had been compromised, and that was not until late in August.

Chairman HENSARLING. My time has expired.

The Chair now recognizes the Ranking Member for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman.

Mr. Smith, I appreciate your being here today. But I want to understand what capacity you are in today. Are you a volunteer? A paid adviser? Do you play any role in the company? Would you please make that clear to me?

Mr. SMITH. Yes. Congresswoman, I am the former Chairman and CEO, 12 years in that role. Today I am sitting here as the former CEO but also someone who has agreed to work with the board.

Ms. WATERS. Are you a volunteer?

Mr. SMITH. Yes, I am not paid.

Ms. WATERS. You are not paid. And so you came today to try and perhaps explain what has taken place. But do you have the ability to talk about what happens going forward and how we can correct the mishaps, the errors, the problems of Equifax? Are you empowered to do that today?

Mr. SMITH. Congresswoman, I have the ability to talk looking forward from my perspective as an individual who was a CEO for 12 years.

Ms. WATERS. But if you make a commitment here today, are you bound by any commitment you make for the company today?

Mr. SMITH. No. Commitments will have to be made by the company themselves.

Ms. WATERS. And so your capacity today is simply to try and explain and take responsibility rather than how we go forward for the future. Is that right?

Mr. SMITH. That is largely correct, Congresswoman. I do have views, again, on paths forward, and I am prepared to discuss those. But commitments will have to be made by the company themselves.

Ms. WATERS. Well, that creates a little bit of a problem for us today. We have such limited time to deal with so many problems. And while I appreciate your taking responsibility and apologizing, your being here today doesn't do much for us in terms of how we are going to move forward and correct the problems of Equifax.

Our consumers are at great risk. As a matter of fact, I have not been able to freeze my credit with Equifax. I can't get through. And you are talking about the improvements that you have made. Are you close enough with the company to know exactly what has been done to be available to consumers?

Mr. SMITH. Congresswoman, yes, I have an understanding that what has been done to make this service level to consumers better. I mentioned in my comments, they have staffed up dramatically on the call centers.

I am told—it is a few days old now—that the backlog of consumers trying to get through and secure their free services has now been emptied and that the flow is now almost instantaneous.

Ms. WATERS. I am not sure about that, and I worry about that.

In addition, I will tell you what else I worry about. How long will consumers be able to get what you describe as free service from Equifax? Is there a time that is going to kick in where they are going to be charged for trying to straighten out whatever problems have been created because of this serious hacking that has been done?

Mr. SMITH. The company has offered five services to every American, not just those impacted.

Ms. WATERS. How many?

Mr. SMITH. Five different services—I can walk through those, if you are interested—which give protection to the consumer and, again, not just those impacted but any U.S. consumer.

Ms. WATERS. For how long?

Mr. SMITH. For 1 year from the time they sign up followed by, in January 2018, under my watch, we started developing this product which is the ability for a consumer to control access to their data for life.

They will have the ability to lock access and unlock when he or she chooses versus us being able to do that on their behalf. And that will be free for life, starting in January 2018. It will be enabled as an application on one's cellphone, for example, so very easy for a consumer to use.

Ms. WATERS. OK. I might have missed part of that. But if one's identity has been stolen, and usually it takes a long time to unravel that, are you going to provide service and protection and assistance to the consumer until that is taken care of?

Mr. SMITH. Yes, Congresswoman. Again, the product we have today, one of the five services we offer today is the ability to lock your access to your file. It will be enhanced in January with easier user interface. That is the most secure way we have to prevent someone from—preventing identity fraud by accessing your credit file. You, as a consumer, determine who accesses it, who does not, and when.

Ms. WATERS. OK. But I am clear. I think what you have said is when one finds oneself in that position that Equifax will provide them with the service and assistance in perpetuity?

Mr. SMITH. For life.

Ms. WATERS. Thank you. I yield back the balance of my time.

Chairman HENSARLING. The gentlelady yields back.

The Chair now recognizes the gentleman from Missouri, Mr. Luetkemeyer, Chairman of our Financial Institutions Subcommittee.

Mr. LUETKEMEYER. Mr. Smith, thank you.

You know, we have—I had a long meeting this past week with some experts in data security and how they can be protected. And one of the comments that was made was that when it comes to information technology budgets, the average company only spends 6 percent on security. Do you know off the top of your head roughly what your company spent for security out of their information technology budget?

Mr. SMITH. Congressman, I do. I think what you are referring to is there is a benchmark on a percent of the IT budget that—

Mr. LUETKEMEYER. Right.

Mr. SMITH —is directed towards security, and 6 percent is the average. IBM, who creates a benchmark, views 10 percent, 14 percent as being best in class. We are in the 12 percent range.

Mr. LUETKEMEYER. OK. Have you put in place or are you aware of new protocols that you have got in place to make sure this never happens again, your company?

Mr. SMITH. Yes. We have implemented multiple protocols over the years, and at the time of the breach step one was the forensic review, step two was remediation plans for short term, medium term, and long term. We have implemented those to make sure we are more secure. We have also engaged a world-class consultant to come out and rethink everything we have done for a long-term plan.

Mr. LUETKEMEYER. OK. As a result of this breach, the exposure is ginormous here, quite frankly. It could, I would imagine, bankrupt your company if something—if this was—for a number of reasons here. Do you have an insurance policy to cover this kind of a breach?

Mr. SMITH. Yes. I have discussed that in the past. We do have a tower of insurance coverage that is common in our world. It is cybersecurity, general liability insurance.

Mr. LUETKEMEYER. OK. So basically the company is protected. Is that right?

Mr. SMITH. Well, there are limits—

There are limits to any coverage you have and limits here as well. I have not disclosed those limits.

Mr. LUETKEMEYER. OK. In your testimony, both written testimony and your verbal testimony a minute ago, you talked about new security processes and you were talking here, creating a public-private partnership to begin a dialog on replacing Social Security numbers as a touchstone for identity verification in this country.

Can you explain what you believe is a public-private partnership with regards to this?

Mr. SMITH. Yes, Congressman. There are two thoughts there: One, the rise and the intensity and severity of cybersecurity incidents around the country and the world is running at a pace that

has never been seen before. And I am convinced there is more we can do in public-private partnership to get ahead of the curve on cybersecurity, not just reacting to it.

Number two is, the more I reflect, think, and talk to experts in the area of cybersecurity, I am convinced there is an opportunity for this partnership between public and private to rethink the concept of a Social Security number, name, date of birth as being the most secure way to identify consumers in the U.S.

It is an instrument that was introduced, as you well know far better than I, back in the 1930s. I think it is time we think about a new way to identify consumers.

Mr. LUETKEMEYER. The Chairman did a good job of discussing the notification problems with regards to this situation. Can you tell me, what do you believe is a better way to notify the individuals? A minute ago you said you basically knew on the 24th that individual data had been breached, and it wasn't until the 7th, which is 2 weeks later, that you really made a notification to the individuals.

Even if you can't get your systems up and running so you can take phone calls, don't you think it would be better to have at least notified the individuals, if not by just a public declaration saying, hey, we have been breached, millions of people's information could have been breached; therefore, all of you who are in our systems need to take precautions and let them on their own take whatever precautions they can rather than wait to find out if they had been hacked or if their information has been breached? Don't you think there would be a better way to go about it?

Mr. SMITH. Congressman, I can reassure you that we took a lot of time to think about the notification process. I will make one point of clarification. On the 24th, the knowledge we had surrounding the breach was still fluid. It was fluid through the 7th. In fact, it was fluid—the forensics did not conclude until Monday of this week.

The other thing I will say is that Mandiant, the cybersecurity forensic experts, recommended that we really prepare ourselves for significant increase, cyber attacks, when you went live with an announcement.

So between the 24th and the 7th, a lot of energy was spent securing wherever we could secure our facilities to give us the best protection against cyber attacks. And also, as you mentioned, Congressman, we had to standup the environment call centers, train people, staff people, pull together the product, the service offering, so a lot of work was being done over those 2 weeks.

Chairman HENSARLING. The time of the gentleman has been expired.

The Chair wishes to advise all members, there is currently a vote taking place on the floor, over 10 minutes left in the vote. We will clear one more member and then declare a recess pending end of votes.

The Chair now recognizes the gentlelady from New York, Mrs. Maloney, Capital Markets Subcommittee Ranking Member.

Mrs. MALONEY. Thank you.

Mr. Smith, as you well know, Americans rely on the three credit bureaus, a select group of companies to safeguard some of our most

sensitive information. And it is because these credit bureaus hold this key personal information that we subject your companies to very rigorous data security standards.

The credit bureaus are subject to the Federal Trade Commission's (FTC's) safeguards rule, which is intended to ensure the security and confidentiality of the information. So we have a law in place that protects—supposedly—against exactly what happened here.

And now we will see if the FTC is willing to enforce it. And if they are not, then we will know that Equifax is clearly above the law. The safeguards rule requires, among other things, that Equifax have an information security program in place that can identify reasonably foreseeable risk to the security of your data and can protect against these risks.

This risk was obviously reasonable, foreseeable, because the Department of Homeland Security literally sent you and the other credit bureaus notice warning you about the exact vulnerability that the hackers exploited. And yet, your security program did not protect against this obviously foreseeable announced risk.

So in my mind, this is the most open and shut violation of the safeguards rule that I have ever seen in the history of this country. So my question to you, Mr. Smith, is, do you believe that Equifax violated the FTC's safeguard rule?

Mr. SMITH. Congresswoman, I understand your point, and it is my understanding we were in compliance with the safeguards rule and that the safeguards rule does not prevent 100 percent against data breaches.

Mrs. MALONEY. How in the world could you let this happen when you were warned by the Homeland Security Department?

My second question, the safeguard rule also requires you to have a patch management system, essentially a system in place to patch security flaws as soon as a fix for the flaw is released. But you have testified that your patch management system failed in this case, even though there was a patch released almost immediately.

Equifax did not implement the patch like it was supposed to. Now, I wrote to the other two credit bureaus a letter about their information security programs to make sure that their systems were fully protected. And one of them wrote me back, Experian. They wrote me a very detailed response, which I would like to submit to the record along with my letter—

Chairman HENSARLING. Without objection.

Mrs. MALONEY—in which they explained that their patch management system functioned correctly. And when they got the notice from Homeland Security they immediately implemented the security patch. They also stated that their patch management system will literally shut down. It won't even work. It shuts down automatically if a patch isn't implemented immediately.

So my question is, why didn't your patch management system automatically shut down your systems when the security patch wasn't implemented? Why was this flaw allowed to go unpatched for months before you noticed it?

Mr. SMITH. Congresswoman, a patch has to be identified. We are routinely notified from—

Mrs. MALONEY. It was identified by the Homeland Security Department when they notified you. You already testified that your person failed to implement it.

Mr. SMITH. Yes. I was referring to, it has to be identified by us not by the outside, either a software manufacturer or, in this case, Department of Homeland Security. As I said in my oral testimony—

Mrs. MALONEY. My time is almost up and I have one more question and I think it is important. You may not know this, Mr. Smith, but it is actually considered best practices in a company with lots of sensitive, personal information to have their chief information security officer have independent business lines that report directly to the CEO and to the board of directors.

But at Equifax, you were using an outdated corporate governance model and had your chief information security officer reporting to the general counsel, not directly to the CEO, and board.

So my question is, why was your chief information security officer not reporting directly to you and the board? And why were you using an old model? Was it because you don't think that information security was important enough to be reported directly to you?

Mr. SMITH. Congresswoman, I don't believe it matters where the chief information security officer reports. It was a priority for me. It was a priority for the board. It is a priority for the company. Having—

Mrs. MALONEY. But it wasn't reported to you or the board. It went to the counsel.

Mr. SMITH. It did not hinder our ability—

Mrs. MALONEY. And it violated best practices for security companies.

Chairman HENSARLING. The time of the gentlelady has expired. There is one vote pending on the floor. The committee stands in recess pending conclusion of that vote.

[Recess.]

Chairman HENSARLING. The committee will come to order.

The Chair now recognizes the gentleman from New Mexico, Mr. Pearce, Chairman of our Terrorism and Illicit Finance Subcommittee for 5 minutes.

Mr. PEARCE. Thank you, Mr. Chairman.

And thank you, Mr. Smith, for being here today.

To get the playing field level underneath us, you would describe the processes at Equifax with regard to outside hacks to be very engaged and pretty professional. We had a human mistake, more or less. Is that kind of correct?

Mr. SMITH. Congressman, I would say, obviously, we committed two very unfortunate errors, the one you mentioned, which—

Mr. PEARCE. I am asking about the overall culture and the approach to security, understanding that you have got a lot of critical data here.

Mr. SMITH. Yes. I would describe the culture and the focus as one that put a top priority on security, yes.

Mr. PEARCE. How much of your time in your 12 years did you spend each day, you say, on cybersecurity?

Mr. SMITH. Congressman, when I first came here we had no cybersecurity organization. I made it a priority 12 years ago to en-

gage consultants to help us scope it out. We went from basically no people to 225.

Mr. PEARCE. So how much time—how knowledgeable are you on the subject?

Mr. SMITH. We had routine reviews.

Mr. PEARCE. No. You. You, you personally.

Mr. SMITH. That is what I am saying.

Mr. PEARCE. So you had routine reviews.

How many times had the Apache Struts been fixed? How many times had it been patched underneath your watch?

Mr. SMITH. Well, we have vulnerabilities in general terms across software. The Apache Struts, the best of my knowledge, this particular open source software, there was one notification on March 8.

Mr. PEARCE. So is the firm still using that software?

Mr. SMITH. It was deployed in two locations. It has been patched.

Mr. PEARCE. But it is still using it? I am not that savvy on all the cyber crimes, but when I hear the Secretary of the Treasury say that 50 percent of his time every day is spent on cyber threats, I was trying to get some sense from you how much of your time every day, because this is probably one of the more critical things. And when I didn't get a very solid answer, then I tend to fall on the side that says that there is a little bit of a lax culture here.

I just Googled Apache Struts to—I just opened the first website, and it talks about something that came out open-source. It was pretty good, but they lost their way about 3 or 4 years ago. To be using a piece of software that the first Google result says 3 out of 5 stars, we probably ought to be looking at better alternatives out there.

And then you have these patches that come out and no one actually responds to them or they—so who made that decision? Where in the hierarchical scheme did that decision not to implement the patch that was suggested, where did that decision come in?

Mr. SMITH. Again, on the 8th of March, the notification came out, as you alluded to from the Department of Homeland Security. A security team sends out a communication to the organization. The patching process, to be clear, to your question, was owned by the chief information officer. It was under his—in his organization.

Mr. PEARCE. Where in this—surely somebody more than just an agent at the field level was tasked with being sure that we don't have any vulnerabilities. Surely it was not that low. So has that decisionmaking stream been made public?

Mr. SMITH. The owner of the process for patching was a direct report to—

Mr. PEARCE. No. I am talking about internally in Equifax. Don't worry about who out there, outside, because you are the one responsible. So is that decision scheme, is the decision process made public, and can we know who? Can we get that information?

Mr. SMITH. Congressman, let me clarify now, if I may. The owner of the process internal to Equifax for the patching, in this case, of Apache Struts or any software that needs to be patched, was an individual who was a direct report to the chief information officer. He is no longer with the company.

Mr. PEARCE. OK. I am about out of time.

Now, your assertion that this is just human error overlooks the fact that you had unencrypted information. Anybody that gets in can read it. It is not encrypted. Is that industry standards that we don't encrypt personally identifiable information (PII)?

Mr. SMITH. Congressman, that is not correct. We use tokenization. We use encryption. We use masking.

Mr. PEARCE. Your testimony a couple days ago answered that you have a lot of information that was just in plain text. I think those all indicate—and the fact that we haven't identified the process—indicate a culture internally that was very lax, in my opinion.

Thank you, Mr. Chairman. I yield back.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentlelady from New York, Ms. Velazquez.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Mr. Smith, in your testimony you stated that you are deeply sorry that this event occurred and that you and the Equifax leadership team have worked tirelessly over the last 2 months to make things right. However, according to an article in Fortune Magazine published on September 26, you are retiring with a payday worth as much as \$90 million.

So my question to you, sir, do you believe it is right for you to walk away with a payday worth \$90 million when the lives of more than 145 million hardworking Americans had been potentially compromised?

Mr. SMITH. Congresswoman, one, again, I do deeply apologize for the breach to those American consumers.

I have heard of this article. I can't reconcile that number. Let me be very clear. I was—

Ms. VELAZQUEZ. How much are you getting in your retirement package?

Mr. SMITH. When I retired, I did announce my retirement. And at that time—so I also told the board back in early September, mid-September that I would not take a bonus going forward. I also told the board that I would be an adviser, unpaid, helping the board and helping the management team for as long—and I asked for nothing beyond what was disclosed in the proxy, and that is a pension that I have accumulated over my career, and that is some equity that I have earned in the past.

Ms. VELAZQUEZ. So you told the Ranking Member that you are here in your capacity as an adviser to Equifax now?

Mr. SMITH. Unpaid.

Ms. VELAZQUEZ. OK. And so are you advising Equifax to set up a compensation fund for impacted consumers to help them rebuild their lives?

Mr. SMITH. Congresswoman, the advice I gave to the board and the management has been followed, and that was to offer five free services for 1 year followed by the ability to lock and prevent identity theft against their credit file for life.

Ms. VELAZQUEZ. But that is not a compensation fund?

Mr. SMITH. Correct.

Ms. VELAZQUEZ. So, Mr. Smith, as Ranking Member of the House Small Business Committee, I am concerned about the impact this historic breach will have on our country's 29 million small busi-

nesses. As you know, the availability of business credit is often inextricably tied to owner's personal credit score.

Last week, Senator Shaheen and I wrote a letter requesting information about Equifax efforts to help small business clients, but we haven't received any response.

So what steps is Equifax taking to educate small businesses and what does it mean for their businesses?

Mr. SMITH. Congresswoman, I understand the question. If we have not responded to your letter, I will make sure that the company does respond in writing to your request.

Specifically to your question, however, if a small businessman or woman was also the proprietor of that company, as an individual, they would be covered by what we are doing for them going forward, offering this free lock product for life. Number two, to clarify if I may, small businesses in America are very important customers of ours.

Ms. VELAZQUEZ. I know that.

Mr. SMITH. And we have told them and others through different functions that they have not been compromised. The data we have on small businesses was not compromised.

Ms. VELAZQUEZ. They were not compromised?

Mr. SMITH. If you are an individual, again, as I said, as a proprietor, you are covered by the services we are offering for free. The small business database that we manage was not compromised.

Ms. VELAZQUEZ. So let me ask you, how is Equifax working with lenders to establish a safe way to check credit scores for borrowers seeking a small business loan?

Mr. SMITH. Again, Congresswoman, if you were a proprietor of that small business, you have the ability to access all the free services that we just discussed.

Ms. VELAZQUEZ. So, this past Monday, it was announced that approximately 2.5 million additional U.S. consumers have been potentially impacted by the breach. Can you assure us that there will be no more discovery of even more consumers who have been potentially impacted as a result of this breach?

Mr. SMITH. It is my understanding that the press release that came out from the company on Monday not only said 2.5 million consumers were impacted additionally but also that the forensic review by Mandiant was now complete.

Ms. VELAZQUEZ. I yield back.

Chairman HENSARLING. The time of the gentlelady has expired.

The Chair now recognizes the gentleman from Michigan, Mr. Huizenga, Chairman of our Capital Markets Subcommittee.

Mr. HUIZENGA. As the Chairman had indicated, I Chair the Capital Markets, Securities, and Investments Subcommittee, where the Securities and Exchange Commission falls under that purview.

You obviously know that, under Sarbanes-Oxley, you have certain duties and responsibilities as a CEO, not just in the running of the company, but in the paperwork filing that has to be filed with organizations like the SEC.

Was data security ever an area you listed as a deficiency in regards to any of these Sarbanes-Oxley requirements?

Mr. SMITH. Congressman, I don't recall it ever being described as a deficiency or filed as a deficiency. It is routinely communicated in Ks and Qs and other means.

Mr. HUIZENGA. But you had internal controls?

Mr. SMITH. Yes.

Mr. HUIZENGA. All right. And presumably you do your analysis on that?

Mr. SMITH. Yes.

Mr. HUIZENGA. So data security was never a part of that?

Mr. SMITH. Not that I—as far as a control issue?

Mr. HUIZENGA. Well, as a control issue or as an area of concern.

Mr. SMITH. It is always viewed as an area of risk for the company. I don't ever recall it being communicated as an area of concern or the lack of controls.

Mr. HUIZENGA. Well, under SEC rules, when you have a material change in the condition of your company, you have to file a form commonly known as 8-K. That 8-K form is there regarding financial condition or prospects and when significant events have occurred. When did you file that 8-K?

Mr. SMITH. I don't recall.

Mr. HUIZENGA. According to my information, it was September 7.

Mr. SMITH. That makes sense. That is the day we went public with the release on the breach itself.

Mr. HUIZENGA. OK. I heard in earlier testimony that you had not been directed by the FBI to withhold information from the public or to slow-walk or to do anything, right? This was not a directive from either the Federal Government through the FBI or any other law enforcement agency or any of your consultants?

Mr. SMITH. Maybe two different questions there. The FBI specifically involved from the second and the very fluid series of communication through, in fact, today even.

Mr. HUIZENGA. But, no, they did not—

Mr. SMITH. Not the FBI. You said the consultants. The consultants did guide us on the communications.

Mr. HUIZENGA. Did those same consultants tell you you better file that 8-K?

Mr. SMITH. The 8-K, as you mentioned, was filed on the 7th.

Mr. HUIZENGA. On the 7th, but you discovered this in July.

Mr. SMITH. Congressman, in all due respect, we did not discover it in July. In July, the 29th and 30th, someone on the security team noticed what they described as suspicious activity. And to put it in perspective, we as a company see millions of suspicious activities against our data from outside every year.

Mr. HUIZENGA. So you had an indicator—let's call it an indicator—July 29th. You hired a consultant, based on your previous testimony, August 2, correct?

Mr. SMITH. That is correct.

Mr. HUIZENGA. OK. So why did it take a month plus, 5 weeks, to file a form with the SEC. And, coupled with that, when did you let your board know about this?

Mr. SMITH. I will answer both of those, if I may.

So, as I talked about in the written testimony and the oral, from the 2nd of August, when Mandiant, the cybersecurity forensic firm, was hired and King & Spalding was hired, a global law firm, very

fluid. They had to rebuild the footsteps of the criminals, where they had been. They had to rebuild the inquiries. It wasn't until late August that there became an indication of a significant—

Mr. HUIZENG. OK. So let's even take that. It still then took 2 weeks for you to file an 8-K, which, in the meantime, you had executives that sold shares. You had the public thinking nothing was wrong—buying and selling shares of Equifax. Would a reasonable shareholder have gotten some of this information and said, "Hey, wait a minute, there is something going on at Equifax, maybe I am not going to purchase that stock"? That seems like that would be a reasonable step for an investor.

Mr. SMITH. And, Congressman, if I may, let me address the point you made on the sale. The sale of the three individuals, individuals, two of them, was back on August 1st.

Mr. HUIZENG. Got it. Regardless, I know it was prefiled. I am not saying that there was necessarily insider information or something nefarious with that. What I am pointing out to you is that, even though your own executives, if they didn't know that this was going on and an 8-K has not been filed, it seems to me that you got the public both coming and going, that you have not only the data, but also the fact that you falsely put your stock out there at a particular price.

So, Mr. Chairman, my time is expired.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from California, Mr. Sherman.

Mr. SHERMAN. Mr. Chairman, I will renew my request that the witness be sworn. When John Stumpf was here his company had adversely affected only 3 or 4 million consumers. We swore in that witness. That is the precedent of this committee in situations like this.

Chairman HENSARLING. The Chair has already spoken to the matter.

Mr. SHERMAN. Mr. Smith, you have made a point that you are an unpaid volunteer for your company. I want to thank you for that service. Aside from \$90 million, you are uncompensated. I know you have disputed the \$90 million figure. So I would ask you to respond for the record in detail how much you have made, pension, stock options, and salary, from Equifax during your term there, and we will see whether the reports of \$90 million are accurate.

Timeline. There is the period from March to July when you should have noticed or your company should have noticed the problem, should have paid attention to the Homeland Security advisory, et cetera, but on—so that is one part of the timeline. Another part starts on July 1, when your chief information officer told you about the attack and that the website was shut down.

Now, there are those in this committee room who have said that the company didn't act immediately on that on July 31. That is not entirely true. In just one day, August 1st, three of your executives sold \$2 million of their stock. That shows an immediate action right after the CIO report. Does your company have any policies on allowing executives to sell stock, getting legal advice before they do so, et cetera, or is it up to each executive to decide how to obey the security laws?

Mr. SMITH. Congressman, let me address both. One, there was never a report issued on the 31st, just to be clear. That was a verbal communication between—

Mr. SHERMAN. Right. But you were told, and the website was shut down. Something pretty significant happened because, the next day, three of your executives sold \$2 million worth of stock. Please answer the question whether your company has a policy of getting approval and legal review before your employees sell stock.

Mr. SMITH. Yes, there is a clearing process.

Mr. SHERMAN. And how would you pass that clearing process, selling the stock just the day after the chief information officer tells the CEO that there has been this data breach?

Mr. SMITH. There is a clearing process required for any section 16 officer. These three were section 16 officers. They all followed the process. The chief—

Mr. SHERMAN. And you don't think the process is broken when it approves the sale of 2 million stocks within 24 hours of when the CEO gets a report of the most enormous data breach—what turned out to be the most important data breach we have had in your industry?

Mr. SMITH. Congressman, I have no indication the process was broken. These three individuals who sold had no knowledge—to the best of my knowledge, had no knowledge—

Mr. SHERMAN. Just your luck.

Now, the initial response of Equifax was to have a website advertised as your way to help consumers. And then, in the website, you tricked consumers—this was the plan—tricked consumers into foregoing their right to sue. Whose idea at the company was it to do that?

Mr. SMITH. The arbitration clause is what you are referring to.

Mr. SHERMAN. Exactly.

Mr. SMITH. That was never intended—when we found out the arbitration clause was in there, within one day, we took it down.

Mr. SHERMAN. You just found out—somehow it popped in, and you didn't know it was there?

Mr. SMITH. It is a standard clause in products where consumers have options to buy product. It was never intended to be in there for the free service. It was removed within 24 hours.

Mr. SHERMAN. After a huge outcry, including many members of this committee.

Now, you have put out press releases telling people that they may be among the 143 million people. Is it the intention of Equifax to send a notice to those whose data were compromised, or is it up to them to go to your difficult-to-use over-burdened website to find out?

Mr. SMITH. We followed what we thought was due process. We sent out press releases, set up a website.

Mr. SHERMAN. How about noticing? Are you going to give notice to the 143 million people? Are you going to send them a letter?

Mr. SMITH. No, sir.

Mr. SHERMAN. Are you going to send them an email?

Mr. SMITH. No, sir.

Mr. SHERMAN. So everybody out there figures there is a two-thirds chance they weren't affected, and they may do nothing, and

you have exposed their data, and you won't give them a notice, not even an email.

Mr. SMITH. 420 million U.S. consumers have come to our website.

Mr. SHERMAN. 420 million U.S. consumers. That is more than the number of people in the country.

Mr. SMITH. Because they have come multiple times.

Mr. SHERMAN. Which means that many haven't come at all. You won't notify people. I yield back.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentlelady from Missouri, Mrs. Wagner, Chairman of our Oversight and Investigations Subcommittee.

Mrs. WAGNER. Thank you, Mr. Chairman.

Mr. Smith, forgive me if I appear a little bit more disturbed or harsh than some of my colleagues, but this issue hits very, very close to home for me. This past year, my tax identity was stolen, and to be frank with you, it has been a complete and utter nightmare. For me this isn't just another data breach. It is a breach of trust.

When we learned that our tax identity was stolen, guess who we turned to for help? That is right: The credit reporting agencies. So, although giving a free year of credit monitoring is a good step, the first step I should say, I don't have much confidence, to be perfectly honest, in the product, sir.

In addition, as the Chairman of the Oversight and Investigations Committee, I will be closely monitoring the additional facts that come out regarding this case, especially those concerning the sale of stocks by executives at Equifax.

Although none of us should, I should say, prejudge before knowing all the facts, and I am sure that the SEC and DOJ will get to the bottom of this. Let me start by asking you this, briefly, Mr. Smith, what would you tell people like me, people who have previously experienced identity theft of some kind and turned to Equifax for help? What do you say to these people who feel completely at a loss for what to do next? How can anyone possibly ever trust—and we have talked about trust here at the committee—this company again, and be confident that they can be protected in the future, please?

Mr. SMITH. Thank you, Congresswoman.

And we are a 118-year old company, and protecting and being a trusted steward of our data is paramount to our ability to gain trust, have trust with consumers and companies around the world. What I would tell consumers is, first, please go to our website, take advantage of the five offerings that we have offered for a year for free. And, second, January 31, when the new lifetime lock product becomes available for free for life, I would strongly recommend that every American go get that product as well.

Mrs. WAGNER. I recently read comments from the Consumer Financial Protection Bureau (CFPB) Director Richard Cordray where he stated his intention to provide accountability concerning the data breach.

As you know, the CFPB began supervising credit reporting agencies on behalf of consumers, I believe, in 2012, but not its cybersecurity systems, which has been left to the FTC. What inter-

actions, sir, did you have with the CFPB prior to the breach regarding cybersecurity?

Mr. SMITH. Congresswoman, I can't recall—obviously, we have been in communication with the CFPB since they have been our regulator, and I personally have been involved in those communications—

Mrs. WAGNER. Prior to the breach, sir?

Mr. SMITH. I can't recall. I was not personally involved with the CFPB regarding cybersecurity myself.

Mrs. WAGNER. Wow. What interactions have you had with them since the breach then?

Mr. SMITH. I have not had interaction with the CFPB since the breach.

Mrs. WAGNER. Wow. Mr. Smith, I did want to take an opportunity to ask you some questions that I have been hearing from my constituents back home. Can you detail what categories of consumer information were accessed during the months-long breach?

Mr. SMITH. Yes, I will give that a shot. We try to be very clear in the series of press releases we have had in the past that the consumers' core credit file, which is their credit history with us, was not compromised. We talked about a database we have, where someone asked on small businesses, we have a database on small business; that was not compromised.

Mrs. WAGNER. What kind of personal identification information specifically?

Mr. SMITH. So, as we have disclosed in press releases, date of birth, name, Social Security number. I think there were 200,000, 209,000 credit cards that were compromised. There is a document, Congresswoman, called a dispute document, where a consumer could dispute that they paid an obligation, take a picture of that, for example, upload that into the system. That was another example that was compromised.

Mrs. WAGNER. Let me ask you this, Mr. Smith, what sort of financial products, for instance, could be opened in my constituents' names if those pieces of data that you just named, for instance, were part of the breach?

Mr. SMITH. Congresswoman, if the consumer takes advantage of the free service and locks their file, no one has access to that file.

Mrs. WAGNER. I thought my file was locked before, after my tax returns were breached, when I reached all of you, so, again, my trust in the product is at an all-time low.

I have several more questions. I will submit them for the record.

Mrs. WAGNER. I thank the Chairman, and I yield back.

Chairman HENSARLING. The gentlelady yields back.

The Chair now recognizes the gentleman from New York, Mr. Meeks.

Mr. MEEKS. Thank you, Mr. Chairman.

Mr. Smith, I agree with the Ranking Member when she initially said, you know, I am here; I am going ask you questions, but I don't know. You know, you are unpaid. You say you are no longer really with the company. You are an unpaid adviser. I don't know what we are going to do with reference to the future. So I am here. I am going to ask you questions. I don't know whether—how long

you are going to be advising them for free or whatever that deal is.

But I know that, when a consumer has a problem, they can't just get out of it in the way that some kind of measly explanation or something of that nature and it is all over with. And you have an extra—or Equifax, your former employer, has a, because of the nature of the business in which they are in, they have a special responsibility in regards to cyber incidents. And I think that it is probably a problem—it is definitely, clearly, a problem with Equifax but probably a bigger problem across the board with all public companies.

There was a PricewaterhouseCoopers survey that found 23 percent of corporate directors did not discuss crisis planning with management and that 38 percent of directors did not discuss their management testing of these crises. And consistent with this data, it seems that Equifax's board and management failed to plan for this crisis, given the company's numerous gaffes, as you have admitted to. Equifax's failure to quickly respond to Homeland Security Department's warning, the company's delayed notification to the public, and the company's arbitration clause misstep, which you acknowledged today and yesterday at the hearing, are just a few examples of Equifax's lack of preparation.

So what I am trying to find out then is, prior to this breach, did Equifax ever adopt a written breach response plan that included a formal process for notifying the public and regulators, or did Equifax merely formulate a cyber crisis plan post the breach?

Second, prior to the breach, did Equifax ever test a crisis plan in anticipation of a cyber breach because you knew the significance of the data that you were here to protect?

And, finally, if you say that there is, can you share with this committee the documents with evidence of Equifax's former cyber crisis response plan?

Mr. SMITH. Congressman, I understand your question, and, yes, we did have and do have written documentation on crisis management, including cyber, obviously being one of the top crises we could face as a company and have faced. So we can reach out to management, have them provide you that crisis management documentation. We will do that.

Mr. MEEKS. And now was there any—my other two questions, was there a written breach response as opposed to the plan of what you would do, something that you say, and did you test it, a crisis plan in anticipation of a breach so that if—like a fire drill, if something should happen, this is what we are going to do, have a plan, have you done that, was that done?

Mr. SMITH. Yes, Congressman, it has been done. The real-life challenge is, when you look at the size of this breach and the fact that we offered it to every American that was a victim or not a victim, the sheer scale of trying to stand up the environment from a technology perspective, hire thousands of people that take weeks to train. You can't just hire 2,000 people, 3,000 people, and expect them to be trained and impactful day one.

As I mentioned in my oral testimony, the team has gotten better each and every day from a technological perspective in the web environment and from the call centers. But, again, I do apologize. You

mentioned a few of the things where we made mistakes early on, but, yes, we do have and have practiced—

Mr. MEEKS. Let me disagree with you. For example, the kind of information that you were to protect, you have to make sure that each and every individual that you hire is prepared. It is like information that we have at the CIA or some other places, protected documents. They can't hire somebody and say: Oh, well we could take a chance and maybe they will learn while they are on the job, and if something happens, it will be OK, and we will just excuse it.

You have got to be sure that you are putting individuals in and have a plan that is going to protect folks because of the nature of the information of which you are given and because of the numbers of people that are dependent upon you to protect their information.

Mr. SMITH. I understand your point.

Mr. PEARCE [presiding]. The gentleman's time has expired.

The Chair now recognizes the gentleman from Wisconsin, Mr. Duffy.

I would recognize the gentleman from Kentucky, Mr. Barr.

Mr. BARR. Mr. Smith, a representative from your company, I think, put it well. He said: Americans expect their mortgages to be approved on time, their auto loan applications to be accepted while they are at the dealership, and the retail credit approved while they are at the counter. Disrupting the miracle of instant credit would hurt the economy.

Can you assess for us the extent to which this breach and this painful experience for the American people, how this may very well disrupt that miracle of instant credit?

Mr. SMITH. Congressman, if we were to get to the point where we allowed consumers, for example, to opt out of the credit system, that would be devastating to the economy. If we don't allow consumers that ability to instantly lock and unlock at the point of underwriting, to your example, that could be devastating for the flow of credit in our economy.

So the intent of the lifetime product that we are going to roll out January 31st gives that consumer the ability—gives them the security level that he or she deserves with the ability to instantly turn on and turn off access to the credit so that flow is uninterrupted.

Mr. BARR. Can you tell me about credit freezes as a solution or maybe not the best solution to problems like this? And what we are talking about here is a consumer telling a credit bureau to not release a credit report unless the consumer contacts the bureau in advance to say otherwise.

Mr. SMITH. The credit freeze itself, Congressman, was something that was born out of regulation in 2003, put into law in 2004, and it is oftentimes confused with a credit lock. So if I may just spend a second and talk about both.

A credit freeze, from a consumer's perspective, largely provides the same amount of protection as a credit lock would. However, States dictate different means of communicating between the consumer and the credit reporting agency that oftentimes can be cumbersome, require phone calls into call centers, can require mailing things back and forth. So that flow that you talked about, a flow of credit, can be disrupted.

The idea of the lock is to make it far more user-friendly, where you can be on your smartphone and literally toggle on to unlock, toggle off to lock. It is far less cumbersome than the freeze.

Mr. BARR. So, as we look at data security, you talked about the many different State laws that you have to navigate. Tell us your view after this painful experience what you think would be a solution. Would a national uniform breach notification rule be better for the American consumer? That is what a lot of us are thinking in the aftermath of this breach.

Mr. SMITH. I have not given that much thought, Congressman, but I will.

Mr. BARR. What about fraud alerts under the Fair Credit Reporting Act, are they sufficient?

Mr. SMITH. I think the most—they do add value. Fraud alerts do add value. Clearly, the monitoring of those alerts gives consumers peace of mind. I think the most significant step forward, Congressman, is this concept where consumers can control who accesses their credit data with a lock, and I think the next step forward there would be to not only have Equifax offer that solution, but imagine a consumer being able to lock and unlock for free-for-life access to all three credit reports, Experian's, TU's, and ours. That gives them the ultimate protection.

Mr. BARR. You went over this a little bit about the steps that you took after learning of the breach and why it took a while for you to notify the American people about the breach, but why did it take so long? I think the average American would expect a more expeditious notification of the compromise of their personal identifiable information.

Mr. SMITH. Congressman, we were driven by a couple of thoughts. One was making sure we were as accurate as possible in who was impacted and who was not. And that just took time. As I alluded to in the oral testimony, that developed over the weeks of mid to late August.

Number two, as I mentioned, Mandiant, the cyber forensic examiner, who is viewed as world class in what they do, had advised us to expect an increased frequency of cyber attacks, and we had to develop plans to make sure we were prepared for those attacks.

Mr. BARR. My time is expiring. Can I just ask you if one of my constituents approaches me with a problem, will you commit to me to working with my office to help any of my constituents whose identification has been compromised?

Mr. SMITH. Congressman, I will ensure the company does that.

Mr. BARR. Thank you.

I yield back.

Chairman HENSARLING [presiding]. The time of the gentleman has expired.

The Chair wishes to alert all members that votes are currently taking place on the floor. The Chair intends to recognize one more member and then go into recess.

The Chair now recognizes the gentleman from Massachusetts, Mr. Capuano, for 5 minutes.

Mr. CAPUANO. Thank you, Mr. Chairman.

Mr. Smith, I want to join my colleagues in saying I don't have a clue why somebody who doesn't work for the company is here. Is

there anybody in the audience that you know of that currently works for Equifax and has the authority to change internal company policies? Is there anyone in the audience that you know of that has that ability?

Mr. SMITH. No, Congressman.

Mr. CAPUANO. No. Well, this is great. Thank you for coming. I appreciate it very much. So, therefore, from this point forward, don't take it personal because I know you can't do anything about it, but I will use you because I am hoping that maybe one or two people back in the company are watching. Maybe not. Probably not because they don't care. But we will find out.

Is it fair and accurate to say that, at any given moment, Equifax has the financial records of approximately 200 million Americans? That is a rough number. Does that sound right?

Mr. SMITH. Congressman, if I may, there are 10,000 people back working at Equifax that do care.

Mr. CAPUANO. Fine. Just answer my question. You can defend the company when they put you back on the payroll. Since you don't represent them, how would you know? So how many average Americans—

Mr. SMITH. I spent 12 years there.

Mr. CAPUANO. Say again?

Mr. SMITH. I spent 12 years there. That is how I know.

Mr. CAPUANO. OK. We will get to that in a minute.

Mr. SMITH. But to answer your question, yes, it is over 200 million U.S. consumers.

Mr. CAPUANO. So 200 million. And your accuracy rate is about 95 percent. Is that—I read that—is that a fair number?

Mr. SMITH. How are you defining "accuracy"?

Mr. CAPUANO. No errors of significant numbers.

Mr. SMITH. You are referring to the credit file itself?

Mr. CAPUANO. Yes.

Mr. SMITH. There was an independent study done a number of years ago. PERC did the study and found that if you defined an error as something that has a negative influence on a consumer's ability to get a loan, either yes goes to no, no goes to yes, interest rate goes up, over 99.9 percent—over 99 percent.

Mr. CAPUANO. Well, I used 95 percent because that is what I read, but the numbers will be close. So you have 200 million records. You get a 95 percent accuracy rate, which means a 5-percent error rate, which means, at any given moment, there are 10 million Americans who you have financial records on and you had 500 service reps. That is 20,000 customers with a problem that your company created per service rep.

Now, you get 145 million—you are ramping up; you are going to hire, give or take, 3,000 service reps—145 million, that leaves 48,000 people with a problem you created—not you, your former company—created per service rep, 48,000. Do you think that is good?

Mr. SMITH. Two points of clarification. I disagree with your math, in all due respect. The math we have is 99 percent. Number two is most of the disputes—if you have an issue with your credit file, we have an online electronic—

Mr. CAPUANO. Let's talk about that for a minute. Let's talk about—I am sure, since you were the CEO in 2014, you are familiar with the case of Miller v. Equifax?

Mr. SMITH. Vaguely.

Mr. CAPUANO. You have heard of that case, I am sure.

Mr. SMITH. Vaguely, yes.

Mr. CAPUANO. And that is a case where the judge found, we didn't find it—as a matter of fact, congratulations on that case because that case was actually determined that you didn't have to pay an \$18 million penalty; you only had to pay a million and a half dollar penalty because that is the most the Constitution allowed, and the judge found that your actions were reprehensible. Those are her words, not mine. And it stated very clearly here that your own expert testified that it is Equifax's policy to investigate and correct files only after a lawsuit is filed, which is why I wanted to talk to somebody in the company to see if they are willing to change that, but since there is nobody here, I guess not.

I just wondered, do you think that is OK? You thought—apparently, you thought that was a good policy in 2014?

Mr. SMITH. Congressman, if a consumer has a dispute on something on his or her credit file, we take that seriously. They have the ability to communicate with us directly electronically or over the phone. We work with the furnisher, the banks, the—

Mr. CAPUANO. In this particular case, you just ignored it. You didn't do anything about it, and the only reason there was a lawsuit is because two people with the same name of Miller, their records got combined, and you refused, after you were proven repeatedly for years, to do anything about it. And it happens all the time.

Every one of us gets complaints from our constituents that your company—not just you; the other two are no different—that your industry treats them like dirt. They can't get student loans. They can't get auto loans. They can't get ATM cards because you won't do anything by your own policies admitted by your own people who used to work for the company that says we don't do anything until you file a lawsuit.

So, here, in my last 13 seconds, I am going to speak to America, and I am going to say for the 145 million people: File a lawsuit and maybe you will get some equity. Otherwise, they are going to keep doing to you what they have been doing to you forever.

Chairman HENSARLING. The time of the gentleman has expired. Votes are pending on the floor. The committee stands in recess.
[Recess.]

Chairman HENSARLING. The committee will come to order.

Without objection, I recognize the Ranking Member for 1 minute.

Ms. WATERS. Thank you very much, Mr. Chairman.

Pursuant to clause 2(j)(1) of rule XI and clause (d)(5) of rule III of the rules of this committee, I am submitting for your consideration a letter signed by all of the Democrats of the Financial Services Committee notifying you of our intent to hold a Democratic hearing, also known as a minority hearing, on the Equifax data breach. I look forward to working with you to determine the date, time, and location of such a hearing.

Chairman HENSARLING. The demand being properly supported by the majority and minority members, the additional hearing day will be scheduled with the concurrence of the Ranking Member, and members will receive notice once the new hearing day is scheduled.

I now recognize the gentleman from California, Mr. Royce, Chairman of our Foreign Affairs Committee.

Mr. ROYCE. Mr. Chairman, thank you.

And I thank Mr. Smith for being here today.

Now, since September the 7th, my office—I am sure all of these offices—have received a lot of angry and anxious phone calls and emails by our constituents. I think one of the things that really stands out is, how could a company that deals in data not protect that data?

I think the answer lies in what your company did not do. You did not protect their personal information. You did not encrypt that data. You did not patch a vulnerability that you were alerted to on March the 8th. You did not disclose the breach to the public until 117 days after it occurred. And then, on top of it, the insider trading allegations only add fuel to that fire.

So let me turn to my questions. Before September 7, who else outside the company and your hired legal counsel and the FBI, who else was made aware of the breach? Was the FTC notified?

Mr. SMITH. Congressman, at the appropriate time, all outside constituents were notified, including the FTC.

Mr. ROYCE. Well, let me ask you this, Mr. Smith: According to media reports, LifeLock executive Fran Rosch was notified before the hack actually became public. According to that individual, he got a call while vacationing in Maine. And I just ask, are you aware of this? Do you know who called Mr. Rosch to give him the heads-up?

Mr. SMITH. No, sir, I am not aware of that.

Mr. ROYCE. Well, according to Bloomberg, armed with information only a handful of people had at the time, Mr. Rosch mobilized the rapid response team. He knew the company would receive an onslaught of calls and signups in the coming days, and I will quote from Bloomberg: He was right. In fact, the phones were ringing off the hook. He bragged that it was bigger than the Anthem breach, bigger than anything they had ever seen before, a tenfold increase in LifeLock customers.

And here's the kicker. Quote from him: "Most are paying the full price rather than discounts,"—I think that means most were paying \$30 instead of \$10—"it is a really incredible response from the market," unquote.

I will tell you what is incredible here: That actually your company profited off the relationship with LifeLock, which is a company to which you provide credit monitoring services. Here is the point I would like to make: LifeLock gets this heads-up. Did Credit Karma or Intersections or the other competitors, did they get similar notice, that you are aware?

Mr. SMITH. Again, Congressman, I am unaware of the LifeLock discussion, let alone anyone else.

Mr. ROYCE. Well, it is fair to say I think that LifeLock benefited from both the breach and the foreknowledge of it. LifeLock's parent

company, Symantec, has seen its stock rise by more than 10 percent since the breach was made public.

Mr. Smith, do you or any current executives at Equifax own stock in Symantec?

Mr. SMITH. I do not, sir.

Mr. ROYCE. Well, what I would like to know is, if you could provide a list of any executives who do, because someone notified them in advance. Someone in the company gave them a heads-up so that they had an opportunity to get the phone banks ready and in advance of anybody else start calling about their service and at a price \$29.99 instead of the \$9.99 discount that obviously was of great benefit to that company. Somebody tipped them off on the inside, and I think it would behoove Equifax to find out who that is. And if you could start by finding out which executives own stock, that might help us get to that answer.

Mr. SMITH. Congressman, your source was Bloomberg. Is that correct?

Mr. ROYCE. That is correct.

Mr. SMITH. We will look into that.

Mr. ROYCE. Very good. I appreciate it.

Yesterday, in the Senate, the question was asked if we had seen any evidence—

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Georgia, Mr. Scott.

Mr. SCOTT. Thank you very much, Mr. Chairman. Good to have you, Chairman.

First of all, I want to make a couple of points very clear. I represent the great State of Georgia. I love Georgia. When this news first came to me, my staff reported it, I immediately wanted to do all I could to make sure that we would be able to make sure that Equifax would be standing tall, that they would be clean. That is my objective as the Congressman from Georgia because, as you said, you represent a legacy of our great State. You are a 128-year-old company. You employ 30,000 people, many of whom are my constituents, many of whom who work and toil in the vineyards at your company, and they are great people doing a great job.

It is important for the American people to know that what we have before us is a despicable, a shameful situation for 145 million American citizens to lose the privacy of their Social Security numbers and all of that, but let it be known that it is the top management—it is you—who is responsible for this.

Now, what I want to do is to be at the front of this spear, to make sure that Equifax regains the confidence and trust of the American people. So my comments here to you, Mr. CEO, are going to be geared to that.

First of all, I want to call, Mr. Chairman, and be the first one to call for an investigation by the Justice Department, by the CFPB, and certainly by the SEC. Now, Mr. Smith, you are leaving this company, but there are others who are going to be there, and we have to make sure that Equifax comes out clean and standing tall.

Now, what disturbs me perhaps more than anything was the timeline. You said that you became knowledgeable about this

breach on July the 31st, but here is what happened: On August 1st, your executives sold \$2 million worth of stock. And not only that, Mr. CEO, former CEO, it was your chief financial officer who led that charge to sell that stock. Now, nobody is going to tell me you are getting information on July 31st and here they go dumping their stock less than 24 hours later. That has to be investigated and cleared if we are going to get the confidence of the American people back. So it is this insider trading; anybody can see that. And I am sure and I hope that your successor—the guy who is going to be taking your place, I hope he is listening. That would be the first thing.

And then the second thing, we need to make sure that these guys who sold that stock, who made \$653,000 in savings from that stock with that inside information, that they pay that money back and that they are fired. 143 million people losing this is no justification. We have got to make sure and you have got to make sure that we clean this mess up.

Now, I want to talk about the other way in which we can do this. You mentioned numerous times that it wasn't the intent of Equifax to include the arbitration piece. Well, now some have it; some don't. That is the next thing that needs to be done. No more of this arbitration clause. When you do things like that, the public will take notice. Our job is to clean this mess up and make sure we bring Equifax back standing tall. We owe that to the American people.

Now, the other thing that I would like finally is my staff informed me that most mortgage lenders pull all three reports from the big three credit reporting agencies: Equifax, TransUnion, and Experian. So, when you talk about this new free lifetime lock product, it is not going to be effective unless everybody does it.

I wish I had more time, but we are going to clean this mess up, and we are going to restore the integrity and trust of the American people.

Chairman HENSARLING. The time of the gentleman has expired. The Chair now recognizes the gentleman from Illinois, Mr. Hultgren.

Mr. HULTGREN. Thank you, Mr. Chairman.

I know most of us have been hearing from our constituents. I certainly have. Marty from Wauconda, Illinois, wrote me, said: Equifax has jeopardized my private information, which I never gave them. Why should I have to do all of the work to monitor my credit? They should have done it for me or pay me to do all this of signing up and freezing my credit reports. They should pay me for my time. Should someone go to jail for this? Do you agree?

James from Spring Grove said: This company, Equifax's careless actions have caused the loss of personal information on a scale never seen before, not due to some new or sophisticated hacking technique, but because they failed to patch their servers for a known problem. Combined with the careless handling of highly sensitive personal information and the likely criminal sales of stocks prior to reporting the breach, their action went far beyond carelessness to negligence. Legislation should be put forward to increase regulations on these entities, not decreased legislation that is proposed. Equifax must be held accountable and liable for all

damage caused by their breach, and all credit reporting firms must be held to much higher standards of information security.

John from Auburn said: In the last 6 months, my private personal information has been lost twice, once by Home Point Financial, my mortgage company, and then again by Equifax. Both companies are offering a limited subscription to identity protection companies. HPF is offering a free year's subscription to protect my ID owned by Experian. Equifax is offering a 1-year member to TrustedID Premier, an Equifax subsidiary, which they acquired in 2013. Seems like a twisted marketing campaign to me, he said. Home Point Financial claims to have lost Social Security numbers, birth dates, driver's license numbers. Many of these lost numbers cannot be changed. What good is a 1-year membership? This data is lost and valuable until I pass away. Is it ethical that a company that loses all my personal data also conveniently owns a service that sells a product and wants me to pay to help protect me from its eventual use? It is time that all these companies are held liable and forced to offer lifetime memberships. Please help us, all of us. This is out of control.

Many other constituents, again concerned, talked with parents of young people whose information has been compromised.

Mr. Smith, when this committee sends questions for the record, of which there will be many, will the response to our questions come from you or from Equifax?

Mr. SMITH. They will come from the company, Congressman.

Mr. HULTGREN. And how should we respond in getting those answers from Equifax?

Mr. SMITH. I will make sure someone from the company reaches out to your staff.

Mr. HULTGREN. That would be great.

Equifax has been investigating the breach now for over 2 months. Has the identity of the hackers been determined?

Mr. SMITH. No, Congressman, it has not. As you know, we are engaged with the FBI, and the FBI is running that investigation for us.

Mr. HULTGREN. Do you have an opinion of whether it will eventually be determined who did it?

Mr. SMITH. I do not.

Mr. HULTGREN. Did outside data security consultants tell Equifax it should delay notifying the public, and if so, why, when, and for how long? What changed that allowed Equifax to notify the public in September?

Mr. SMITH. Again, it was trying to balance—it was a team effort, and it relied upon the input from our outside forensic examiner, a global law firm that we talked about, and our team. It was trying to balance accuracy, clarity, transparency with the urgency of contacting the consumers.

Mr. HULTGREN. Was an event like this in the scope and scale contemplated by your security staff in a preventable sense? Did a playbook exist for responding to a material breach of Equifax's PII database?

Mr. SMITH. Yes. There was a crisis management process that we have had in place for quite some time, and a data breach is one of the crisis examples that we practice routinely.

Mr. HULTGREN. It just doesn't appear like you were ready for it, and that is our question, of the incredible delays. You have heard from my constituents. This is just a small sampling of incredible frustration, fear that their information has been compromised, and they don't know if it is ever going to change. Echoing what one of them said, this is information you can't go back and change. You can't go back and get a new birth date or a new Social Security number.

If Equifax had wished to notify the public within let's say 1 week of discovering the breach, would it have been capable of doing so? Could it have had both the resources and the plan in place to do so? Why or why not?

Mr. SMITH. Congressman, we moved with haste. As I mentioned in my oral testimony and the written testimony, it wasn't until late August that we got a sense for the size and scope of the breach, and even that was continuing to move. We moved as quickly as possible thereafter.

Mr. HULTGREN. Has there been any uptick in identity theft or fraud since the breach?

Mr. SMITH. Not that I am aware of.

Mr. HULTGREN. Would you expect something like that to occur, and why might there not be an uptick yet?

Mr. SMITH. If consumers take advantage of the services that we are offering, Congressman, to lock their file, that will give them great protection.

Mr. HULTGREN. Obviously, there is a concern when still those kinds of same entities are involved.

My time has expired. I yield back.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Illinois, Mr. Foster.

Mr. FOSTER. Thank you, Mr. Chairman.

What I would like to talk about are things that Congress should have done or can do at this point that would have prevented this. And, what that means is that you would have needed a team of really smart highly motivated people looking every day for any security flaw, which you obviously did not have in place.

And one way to make that happen is by making it a requirement that you actually carry enough insurance to make customers whole when this thing happens. It is my understanding that statutory damages for a breach like this are roughly \$1,000 per person, which means that the total potential liability for 140 million people is \$140 billion, more than 10 times the market capitalization of Equifax. You clearly can never self-insure, or at least a company with your business model could never self-insure.

On the other hand, some of these have settled for a lot more—a lot less, just a few dollars per person for some data breach instances. So it is not clear what it should be.

My first question is, what would you personally for yourself or one of your family want as remuneration for having your private information up for sale on the dark web?

Mr. SMITH. Congressman, the suite of services we are providing for free in some cases—

Mr. FOSTER. No. I am saying if I came up to you and said, "I want to publish your information on the dark web," would you do it for \$1,000, personally, just personally or on behalf of members of your family?

Mr. SMITH. No, sir.

Mr. FOSTER. No, you would not. OK. \$10,000? \$100,000? Everyone has that number, but it is well north of a few dollars per person. OK. But that is sort of what is happening. Without even having a negotiation, we are having this pain inflicted on people.

Let's just stick with the \$1,000 a person, just the statutory number on there. Oh, plus punitive damages. And so, now, if Congress were to require that any company like yours that held information for people without asking them necessarily to opt in, that you had a requirement that you would hold enough insurance to make them whole if there was a massive data breach, that would be a very expensive insurance policy, correct? Right?

Now, you indicated earlier that you had not disclosed how much insurance against data breach you are actually carrying. Is that correct? And you don't intend to tell us that?

Mr. SMITH. That is correct.

Mr. FOSTER. That is correct. OK. Is it fair to say that it is not enough to cover \$140 billion, \$1,000-per-customer type liability? Is it less than that? Are you comfortable saying that?

Mr. SMITH. Yes, it is less than that.

Mr. FOSTER. OK. And so it is likely that many customers may end up getting less than they think really their actual damages are.

Have you thought through, say, how much per hour the average customer would charge someone to just sit on hold waiting to try to get attention to getting their credit unfrozen?

Mr. SMITH. Remember, Congressman, one of the offers we have to consumers is an insurance policy. You are aware of that? We offer five different services for free. One is, if a consumer has lost expenses in trying to get their credit repaired, trying to take time off of work, up to a million dollars.

Mr. FOSTER. OK. But I am trying to understand under what conditions you would have assembled a team, either yourself or an insurance carrier, assembled a team that would have prevented this. If you would have tens of billions of dollars of coverage on this, I imagine that would have funded a very aggressive team of people who would, every time a patch came out, they would say, oh, boy, let's go and try to figure out if you have applied that patch. And they would be looking at your source code for everything that an insurance company that was offering that kind of coverage would demand. And I was wondering if you think there is a possible way that we can actually prevent this in the future.

Mr. SMITH. Congressman, we have notifications routinely every year for patches. This is a very unfortunate mistake. I mentioned the mistake; I apologized for it. The insurance approach is not the solution. It is preventing the human error and the technological error that occurred.

Mr. FOSTER. But there will always be human errors, and what you need is a red team who sits there and looks for human errors and flags them immediately. And this has to be a very expert team.

Nothing short of that is going to rapidly catch the kind of human errors that will naturally happen. So, anyway, this is one of the things I am looking at, because it is the only free market solution that I think has a chance of preventing this in the future. Thank you.

Chairman HENSARLING. The time of the gentleman has expired. The Chair now recognizes the gentleman from Colorado, Mr. Tipton.

Mr. TIPTON. Thank you, Mr. Chairman.

Mr. Smith, I appreciate you being here. I did want to follow up on some previous questions that I had heard. The question was around whether or not you had protocols in place to be able to actually address whether or not the information was being reported properly internally, but then also to the government entities that are responsible for oversight.

And I did not hear you respond to the answer whether or not you have written protocols in place to be able to have a timeline to be able to make sure that the governing bodies overseeing you are notified in a timely manner. Would you address that?

Mr. SMITH. Yes, Congressman. Thank you for that question. Yes, there were protocols in place. The protocols started with when the security individual saw suspicious activity. Protocol No. 1, he or she shut down the particular portal, started the internal investigation, followed by the traditional protocol that they followed, which is to notify and engage outside cyber forensic auditor Mandiant, engage outside counsel to help us with the investigation, and then protocols followed throughout all the way to the time of notifying the regulators, AGs, and the consumers.

Mr. TIPTON. Looking forward, to try and be a little more solutions-oriented—I understand and appreciate the comments that you have made regretting what took place—are there protocols, are there actions that this Congress might be taking, in terms of some of the regulatory bodies, to be able to incentivize earlier action, earlier notification, not only to the governing bodies but also to the consumers as well that we ought to be looking at?

Mr. SMITH. Congressman, the one thing I mentioned before I would love to see both Congress and companies tackle is the concept of, is there a better way to identify consumers in America other than SSN? It is unfortunate the number of breaches that have occurred over the years has exposed so many SSNs that we are all vulnerable to that. So I would love to see us engage in that discussion.

Mr. TIPTON. Well, in terms of internally, there are some independent—I believe The Wall Street Journal had noted independent groups that analyzed the vulnerability of you, of Equifax, in terms of what you are going to be dealing with.

Do you look at that sort of analysis, and who is responsible for identifying that and taking it seriously, to see that patches aren't needed, but we are being proactive to make sure that the breaches do not take place?

Mr. SMITH. Yes. We routinely bring in outside consultants, advisers to help us check, double-check, rethink tactical steps we can take as we have taken since the breach as well as long-term strategic steps we can take to make sure we are more secure.

Mr. TIPTON. Great. Thank you.

Mr. Chairman, those are the questions that I had. I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Maryland, Mr. Delaney.

Mr. DELANEY. Thank you, Mr. Chairman.

Thank you, Mr. Smith, for being with us here today.

I have a couple of questions about how you interacted or how your board interacted around this matter generally. So it says in your testimony that you became aware of the information on August 11, but that you notified the lead member of the board of directors, Mark Feidler, on August 22. Did you have any conversations with other board members before that?

Mr. SMITH. Let me clarify, if I may. The first debriefing I had of any significance was on the 17th of August. That included Mandiant.

Mr. DELANEY. Got it. Sorry. But between the 17th and the 22nd, did you speak to any other board members?

Mr. SMITH. On the 22nd of August was the first discussion with the lead director.

Mr. DELANEY. What about other board members?

Mr. SMITH. The 24th and 25th, we had two board meetings where the entire board was updated.

Mr. DELANEY. Is it normal to wait this long to convene your board when a matter of this scale has occurred?

Mr. SMITH. The data was fluid, moving, developing each and every day, and I felt that was an appropriate timeline.

Mr. DELANEY. Under the Sarbanes-Oxley requirements for public companies as it relates to their internal controls, was cybersecurity or data breaches ever considered as part of the board of directors and the audit committee?

Mr. SMITH. In what way?

Mr. DELANEY. Well, I ran two public companies, and I used to have to sit down with my management team and get certificates where they would assure me that things were being done in accordance with our procedures. And then the audit committee would review these things so that they could do their job under the requirements of the law.

So, in that process, I assume you engaged in a similar process at your company.

Mr. SMITH. We had two ways to engage as it relates to security with the board of directors. One was at the entire board level routinely through a device we call ERM, enterprise risk management. At the top of that list was cybersecurity. Also go through deep dives with the board of directors on security risks.

The second means of communicating with the board was through a committee we have called the Technology Committee. The Technology Committee is comprised of individuals, some of which have a deep understanding of security. They would go into details of our security efforts as well.

Mr. DELANEY. If you were to put the board's time in a pie chart representing 100 percent of the time they spent on matters related to the company, what percentage of their time would you say was spent on thinking about cybersecurity risk and data breaches?

Mr. SMITH. I would be guessing if I were to make that—take a stab at that.

Mr. DELANEY. Did you regularly have full discussions around the board table about this potential risk? You identify it as a risk factor in your financial statements—I mean, in your 10K.

Mr. SMITH. Absolutely.

Mr. DELANEY. So would you say 5 percent, 10 percent, 15 percent, 1 percent?

Mr. SMITH. Congressman—

Mr. DELANEY. You chaired the board so you have a sense as to what occurred in the board meeting. I assume you set the agenda. So, on the agenda, was there a regular item about cybersecurity or data breaches in every board meeting?

Mr. SMITH. Not in every board meeting, but routinely throughout the year, through committee meetings and through board meetings, the board was apprised.

Mr. DELANEY. Which committees had responsibility for this? The Audit Committee?

Mr. SMITH. As I just mentioned, the Technology Committee.

Mr. DELANEY. The technology. So the Audit Committee didn't.

Mr. SMITH. The Audit Committee would have purview as well. The entire board would have a view. But the Technology Committee—we are a technology company—

Mr. DELANEY. Right.

Mr. SMITH. —was responsible for oversight of security and technology at the board level.

Mr. DELANEY. Would the technology company make a presentation at every board meeting?

Mr. SMITH. Yes.

Mr. DELANEY. Were there discussions about the technology budget at the board level, about whether it was adequate in the area of cybersecurity?

Mr. SMITH. The Technology Committee, Congressman, would approve the technology budget every year.

Mr. DELANEY. Got it. And they bring it to the board for approval, or they just do it at the committee level?

Mr. SMITH. Yes.

Mr. DELANEY. In your opinion, how mindful was the board before this event occurred as to the likelihood of a risk like this?

Mr. SMITH. Very mindful.

Mr. DELANEY. So you would say that your board spent considerable time trying to get to the bottom of—

Mr. SMITH. The board understands, Congressman—it is a data company, to your point—that data security is the number one risk we have and took that very seriously.

Mr. DELANEY. And as part of the disclosure statements that you received as a CEO, where your direct reports would certify that things were being done correctly, did one of those certificates include some mention of the cyber risk and the data breach, the potential for data breach and assurances that the systems were in place?

Mr. SMITH. We disclose in every K and every Q that security is a risk and one risk we face.

Mr. DELANEY. Got it. Got it. And have you had other significant events in the company where you notified your board of these problems the day they happened?

Mr. SMITH. Have we ever notified the board of a security risk in the past?

Mr. DELANEY. So let's say you had analyst expectations as to your earnings and realized during the quarter you were going to miss them, would you call the board, your lead director that day and notify them, or would you wait 4 or 5 days?

Mr. SMITH. If there were risks to our financials to a particular quarter, we would notify the board.

Mr. DELANEY. Sooner than 5 days?

Mr. SMITH. We have never had to do that in my time there.

Chairman HENSARLING. The time of the gentleman has expired. The Chair now recognizes the gentleman from North Carolina, Mr. Pittenger.

Mr. PITTENGER. Thank you, Mr. Chairman.

Mr. Smith, we are addressing a very egregious concern in our country. Obviously, we have major threats, national security threats affecting our financial systems, our infrastructure, our government. The private sector spends hundreds of millions of dollars every year regarding cybersecurity measures, as well as energy companies and other institutions.

Today, we are aware that not just the 143 million consumers' personal information was exploited, but in addition, there are now another 2-1/2 million people that have been affected by this initial account. Can you assure us that the 2-1/2 million are the last Americans whose data has been compromised?

Mr. SMITH. Congressman, can you repeat that last part of your question? I missed that.

Mr. PITTENGER. Can you assure that the 2-1/2 million additional people who have been reported that their data has been compromised, is that the last?

Mr. SMITH. I am sorry. I missed that.

Yes, it is my understanding from Mandiant, the forensic experts, that, one, movement from the time you announce to the final conclusion is not unusual.

And number two is, while I have not had a chance to read the press release myself, it is my understanding that, on Monday, when it came out from the company, it said that the forensic review is, in fact, complete.

Mr. PITTENGER. Yes, sir. Prior to the security breach, did Equifax, in your opinion, have preventive measures in place to combat a data breach of this magnitude?

Mr. SMITH. Well, obviously, a breach of this magnitude would not have occurred if everything was in place.

Mr. PITTENGER. Elaborate with us on additional measures that you believe could be put in place at this time.

Mr. SMITH. Congressman, many have. From the time of the announcement, actually before the announcement, we engaged experts to help us increase monitoring, penetration techniques, what they call white-labeling of IP addresses. A variety of things were put in place before the announcement on September 7. Those continue. We had 30-day plans, 60-day plans, 90-day plans. And as I

was getting ready to step aside, we engaged a topnotch consulting firm to help us rethink our entire strategy for security.

Mr. PITTENGER. Do you actively engage in testing these databases for vulnerabilities?

Mr. SMITH. Yes, we do.

Mr. PITTENGER. Do you use third party, or do you do this in-house?

Mr. SMITH. As I was just mentioning, we do both.

Mr. PITTENGER. OK. Could you please explain the process or standards by which Equifax has stored consumers' personal information?

Mr. SMITH. Could you say that again, please?

Mr. PITTENGER. I would like you to explain the process or the standards by which Equifax has stored consumers' personal information.

Mr. SMITH. Standards. I would say there are a variety of techniques used, from a security perspective. There are layers of security techniques we use. There is—I think it was mentioned or asked earlier.

Mr. PITTENGER. Is there an encryption procedure in place?

Mr. SMITH. That is where I was going. There is encryption. There is tokenization. There is masking. There are layers and different ways to secure that data.

Mr. PITTENGER. Do you feel like that there was adequate encryption in place? Could you have done more to prevent what occurred?

Mr. SMITH. If we could have prevented the human error, if we could have prevented the scanner from not finding this, that would have stopped this issue, yes.

Mr. PITTENGER. So there was a thorough encryption process in place, in your opinion?

Mr. SMITH. Again, there are different techniques used in different areas, and encryption is only one of them.

Mr. PITTENGER. Moving forward, how do you and the rest of the leadership at Equifax plan to regain the trust of our consumers?

Mr. SMITH. By making it right for the consumers.

Mr. PITTENGER. Well, I thank you for coming. This no doubt is probably the hardest time in your life, but it is a much harder time for the American people whose data was exploited, and we are here on their behalf.

Mr. SMITH. I agree. Thank you.

Mr. PITTENGER. I yield my time.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Missouri, Mr. Clay, for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

And, Mr. Smith, thank you for being here. More than 2-1/2 million Missourians had their information exposed in the Equifax breach, and they will likely be impacted by it for years to come.

Can you share with this committee and the American public what types of activity that these people can expect whose identity has been compromised and tell them what kind of activity they can expect from the thieves that took their personal information? Because most Americans have never had identity theft occur to them.

Can you give us some examples of what they can expect over the next year?

Mr. SMITH. Congressman, I would answer that two ways. One, we have offered a comprehensive suite of services free to all Americans to protect their identity, to your point. That is those five different things we talked about earlier. The important point there is I have offered that—or we have offered that to every American.

So, regardless of them being impacted by our breach or not—they could have been impacted by the OPM breach. They could have been impacted by the Anthem breach, Home Depot. We are covering all Americans with a suite of products.

Mr. CLAY. But describe for this committee and the American public the hellish nightmare they are about to go through when they find out that the IRS, that someone has filed taxes in their name to get a refund by the IRS, or that someone has gotten a credit card in their name.

Mr. SMITH. So, Congressman, one of the products we are offering, as we talked about, is the lock. If a consumer takes that lock, locks access to their file, no one can open up a credit card in his or her name, as an example.

Mr. CLAY. Equifax has offered consumers a year free of credit monitoring services, free credit freezes now, and a promise to provide a better product in several months described as, quote, “lock,” unquote on consumers’ credit reports.

At an Energy and Commerce Committee hearing held earlier this week, you stated that credit freezes and credit locks are, quote, “virtually, if not exactly, the same,” end quote. If the protections these products afford to consumers are the same, what is the need for the new term?

Mr. SMITH. Congressman, lock was introduced through regulation in 2003 and 2004. What I was referring to in the quote you mentioned is the protection to the consumer is largely the same. The difference is the ability to freeze and unfreeze can be very cumbersome and is dictated at the State level. The lock product coming out in January 2018 will be very user-friendly. A consumer can lock and unlock from their iPhone. That is the difference.

Mr. CLAY. OK. So, because security freezes are covered by State law, if something goes wrong, for example, if credit accounts are fraudulently accessed, will consumers be protected from financial liability?

Mr. SMITH. Congressman, again, locking or freezing protects the consumer from someone accessing their credit file to access credit, to rent an apartment. It is a secure way to protect their credit file.

Mr. CLAY. OK. Yes, but I am talking about the activity that occurs when they are compromised, when their identity is compromised. What kind of comfort can you give these people? Can you tell them anything, that your company will work with them to resolve this or what?

Mr. SMITH. Yes. Again, we are working with consumers impacted and not impacted. We are offering five different products today for free, followed by the lifetime ability to lock and unlock your file for free. That should give them comfort, an ability to stop people from opening and accessing their credit file.

Mr. CLAY. OK. Do you agree that steering consumers into a product that is covered by a contractual agreement with your company when the product you say is the same that is already covered by many State laws raises some concerns?

Mr. SMITH. No, sir, I do not. The freeze is still our product. The way a consumer gets access to freezing and unfreezing is set by State law.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentlelady from Utah, Mrs. Love.

Mrs. LOVE. Thank you.

Estimates are that about 60 percent of adults, U.S. population, is affected by the breach. If you extrapolate the information to Utah, that is about 1.43 million Utahns that are potentially affected.

So my question is, what sort of financial products could be opened in my constituents' names if their data was part of the breach?

Mr. SMITH. Congresswoman, two things: One, if you are interested, we have the data of those that were a victim of the criminal hack by State level. If that would be interesting to you, we can get that to your staff.

Mrs. LOVE. I would love that. That would be great. But I am still asking what type—if they were affected, what type of products could be opened in their names?

Mr. SMITH. Well, if they signed up for, as many, many have since the breach, with the lock product, the ability to lock their file so no one can access it, so no one can open a credit card, get a car loan, get a home equity loan, get a mortgage, the lock prevents that from happening.

Mrs. LOVE. So, if they didn't get a lock and they are still—if they didn't get a lock, so that means credit cards could be opened in their name, other things could be opened. I just want to get a list of things that they need to look out for.

Mr. SMITH. We monitor. We are offering a monitoring service as well. So, if you are a victim of the criminal attack, we will send you notifications if there is suspicious activity on your file.

Mrs. LOVE. Have there been any upticks in identity theft or fraud since the breach?

Mr. SMITH. It was asked earlier. Not that I am aware of, no.

Mrs. LOVE. Not that you are aware of, OK.

Mr. SMITH. You mean since the breach?

Mrs. LOVE. Yes.

Mr. SMITH. Yes, not that I am aware of.

Mrs. LOVE. How would you know? How do you know?

Mr. SMITH. We have fraudulent flags on files.

Mrs. LOVE. OK. And when would you expect to see an uptick? Because usually some of these things take time. So, if there were to be some upticks, when would you expect to see some of those?

Mr. SMITH. It depends. There are some out there that say that the Social Security numbers, which is the piece of the PII that we focus the most on here, have been out in the public domain hacked in the past for quite some time.

Mrs. LOVE. OK. So, for my constituents that were impacted, how long should they expect to remain concerned about the potential impact on their credit files or identity?

Mr. SMITH. They should always be vigilant and looking at the monitoring products that we offer. And, again, I go back, the first thing they should do is lock their file. If they lock their file, they are going to rest better.

Mrs. LOVE. OK. So, in terms of—I am trying to—what I am trying to do is to give a clear vision to people who are watching what they need to do. I understand locking their file, and some people who are watching that today can do that. But in the meantime, I need to give them things to look out for, what to look out for either before they do that or, over the years what they need to be aware of.

Mr. SMITH. Maybe I will try to answer it this way: If the consumers in Utah or anywhere in America take advantage of the free service, whether you are a victim or not, of the five offerings we have—one is monitoring of all three credit bureaus' files. That is the first thing they should do. We do that for them for free. The second thing is access your credit file through us to look at it for suspicious activity. Three is we offer a dark web scanning service. We go out there for you and scan the dark web for activity. Four is we have the ability to lock the product for free. And there is a fifth one. I forget what the fifth one is.

Those five products should give the U.S. consumer, the Utah consumer far more comfort, followed by January of next year the lifetime lock.

Mrs. LOVE. So can you explain, and I may have missed this, can you explain the difference between a credit lock and a credit freeze?

Mr. SMITH. Yes. The credit freeze was enacted as part of FACTA back in 2003, passed into law at the State level. Each individual State passed it into law 2005—2004. The difference is the ability and the means by which a consumer communicates to us, TransUnion, and Experian, versus the lock, which will be an application enabled on and off, much more user-friendly, much quicker for the consumer.

Mrs. LOVE. OK. And I just want to reiterate one more thing that was brought up by the Ranking Member, that you are committing to work with people who may have been or have been affected or may have had their identity taken and used for their lifetime?

Mr. SMITH. Yes. We are offering every citizen, American citizen a lifetime lock, the ability to lock and unlock for life.

Mrs. LOVE. OK. Thank you. I yield back.

Chairman HENSARLING. The gentlelady yields back.

The Chair now recognizes the gentleman from New Jersey, Mr. Gottheimer.

Mr. GOTTHEIMER. Thank you, Mr. Chairman.

And, Mr. Smith, thank you for being here today.

As a former Microsoft executive, I have an appreciation for corporate integrity and where the buck stops. I get that issues come up all the time. It is how you handle them, of course, when they do come up.

And it seems to me your response has been more of an Equiscam than an Equifix on too many of these accounts that have been brought up today. And if you are going to take 4 to 5 weeks to tell consumers what happened, I just don't understand where the gap was in terms of putting information together so that you can respond well.

One, and if you can help me here, out of the 145 million consumers impacted, only 7.5 million have signed up for monitoring services is my understanding. Why do you think only 10 percent have, and why not just auto-opt everyone in since you have their information?

Mr. SMITH. It is illegal. It requires the consent of the consumer.

Mr. GOTTHEIMER. Can you reach out—since you know their addresses and information and many of their emails, since, obviously, we know that you have them, why not reach out to them and send them a letter and say, “Would you be interested in this”?

Mr. SMITH. I may have mentioned in my oral testimony, Congressman, that the awareness is at record highs for breaches. Over 400 million consumers have come to visit. They know.

Mr. GOTTHEIMER. Couldn't you send out or would you be against sending a letter to them to give them information so they know, so hopefully we can get more people signed up?

Mr. SMITH. Again, I think they do know.

Mr. GOTTHEIMER. I am sorry, is that a no, you are not willing to do that?

Mr. SMITH. I was going to answer.

Mr. GOTTHEIMER. Please.

Mr. SMITH. So we sent the press release out to notify. We set up the website. Phone numbers. We followed State law where that was required for local advertisement to create the awareness.

The 2.5 million that was mentioned earlier that the company released of additional victims of this crime, on Monday, those individuals, because of the fear of false positives, were notified via email or will be notified via email.

Mr. GOTTHEIMER. So the rest, the 143 or 144 million plus, you will not be willing to reach out to?

Mr. SMITH. We follow the process that is legal, acceptable, and common for this size, yes.

Mr. GOTTHEIMER. Thank you for your answer.

What is being done to resolve the problems with your website—I am sure you have read about them, heard about them, I have experienced them—to make them more stable, eliminate bad and confusing links, and to make essential information more accessible? And also I know people got emails saying, “Sorry, we can't get to this for a few weeks.” I think you have caught up there is my understanding. But what do you do about the website crashing?

Mr. SMITH. Yes, it has come a long way. Again, the volume was overwhelming, as I noted in my oral testimony early on. They have taken the right steps to fix that experience. It is my understanding that the experience at the call centers and the website are far, far better today than they were September 7.

Mr. GOTTHEIMER. Yes. And I think we should keep bringing them to your attention because when they crash, you know, people get

even more anxiety. So, if you can please—there are a lot of resources out there that can help you with that.

Can you verify for me that the arbitration clauses or other legal liability limitations are not being included in Equifax's offerings of credit monitoring, credit freezes, credit locks, and identity theft insurance?

Mr. SMITH. Congressman, the arbitration clause is a standard clause in products that we sell to consumers, and consumers have the right not to buy a product from us, but go somewhere else to get that product. The intent was never to have the arbitration clause apply to the free offerings. We were made aware of that and, within 24 hours, took that arbitration clause off.

Mr. GOTTHEIMER. Good. Thank you.

Equifax is claiming, as you have talked about, to provide a million dollars in insurance coverage for identity theft to affected consumers, but the coverage has numerous limitations and exceptions, and the timeframe for covered loss can be unclear to some people.

Does Equifax believe that this insurance is in lieu of reimbursing customers for their actual losses, and can you make clear to people the limitations of the insurance, because I know that it doesn't cover everything?

Mr. SMITH. That is correct. It is expenses incurred. I think, again, the five services we are offering upfront, combined with the lifetime ability to lock your file, are the right steps for the company to take for the consumers.

Mr. GOTTHEIMER. Yes. I think that this is a big issue because you see a lot of these insurance companies and they provide this coverage, but it really doesn't cover what people think. And so, as liability occurs, there are holes.

I am sure you have heard about the phone call wait times. I know one of my constituents wrote in they were on the phone an hour the other day, and others have called in about it being 45 minutes. How are we doing there? What has the improvement been?

Mr. SMITH. It has been dramatic. We have gone from 500 call center people to over I think it was 2,700 was the last number I have heard of trained people to handle those phone calls.

Mr. GOTTHEIMER. Do you know the wait time now?

Mr. SMITH. It has come down significantly. I don't have the exact number. I saw the data earlier in the week, Congressman.

Mr. GOTTHEIMER. Is that information you can get to us, just a sense of where you are now, average waits?

Mr. SMITH. Yes.

Mr. GOTTHEIMER. It seems to me it shouldn't be more than a couple minutes—obviously, there is huge capacity out there to add bodies and given how people have huge anxiety over this issue.

I think that is the key here in my 8 seconds. People can't feel like this is an Equiscam. They have to feel like you are fixing things for them and making their lives better, given that their credit is hugely up for question now in front of many eyes. So thank you so much for your time.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Arkansas, Mr. Hill.

Mr. HILL. I thank the Chairman.

Thank you, Mr. Smith, for coming in today. I appreciate your chance to visit with the committees on Capitol Hill about this important issue.

This is something my family understands. We have had the pleasure of being in the OPM breach, the IRS breach, and couldn't file our returns on time a year ago. And now I see we are gratified to receive your email about also being in the Equifax breach. So I can feel the frustration for a lot of Americans.

And in Arkansas, according to our attorney general, Leslie Rutledge, 1.2 million people in Arkansas, some 40 percent of the population of the State, are covered by the announced breach by Equifax. So we do appreciate our chance to sit down and ask the hard questions that we are being asked by our constituents.

I want to follow up on some of the line of questioning and start out just talking about the management practices at Equifax, if I could. Did you have a weekly executive management meeting with your top officers, your direct reports?

Mr. SMITH. Are you referring to post-breach?

Mr. HILL. No, just generally. As a general practice at Equifax, did you have an executive management meeting with your direct reports on a regular basis? Maybe I shouldn't have said weekly. But did you?

Mr. SMITH. Yes, Congressman. We had routine operating mechanics to run the company. Some might be weekly. Some might be every other week. Some might be monthly. Some might be quarterly.

Mr. HILL. Right. It is a mix, and I am sure a mix of levels of people in the company came, depending on the topic. But in your direct report meetings, would Mr. Gamble be in those meetings at that smaller group on whatever frequency it was?

Mr. SMITH. It would depend on the meeting itself, but largely, yes. He would be involved in many of the meetings we had as a CFO.

Mr. HILL. And Mr. Loughran, who is the president of information systems, as well, would he have been in that meeting?

Mr. SMITH. Again, I have got 12 to 13 direct reports—

Mr. HILL. Is he one of them? Is he a direct report?

Mr. SMITH. Yes. So the three you are probably going to, and Rudy Ploder would be the third.

Mr. HILL. Right.

Mr. SMITH. All three are direct reports to me. All three would be in most of the meetings we would have at the—

Mr. HILL. And then Mr. Kelley as well, as the chief legal officer?

Mr. SMITH. Again, there are 13 or 14 individuals, yes.

Mr. HILL. I am just curious. In that meeting of your trusted advisers at the top echelon of the company, between March 8 and the end of July, did this topic come up among that group?

Mr. SMITH. No, sir, it did not.

Mr. HILL. And in that period between March 8 and end of July, when did you really feel or you were told that it was a serious business challenge?

Mr. SMITH. It wasn't until—the detailed review we had is noted I think in written testimony on the 17th of August with the

cybersecurity forensic team Mandiant, the outside legal team of King & Spalding, my team. It was the 17th of August was the first deep dive.

Mr. HILL. Let me turn and talk about the section 16 officers in the company. I am sure the people we just talked about are all section 16 officers. The chief legal officer, the CFO, yourself, the president of information systems, Mr. Loughran, are all section 16 officers.

Mr. SMITH. That is correct.

Mr. HILL. And your 12b5-1 plan, I assume that is all holdings, and then any in-the-money options would be covered by somebody's preplan to sell stock?

Mr. SMITH. The 10b5-1 plan?

Mr. HILL. Yes.

Mr. SMITH. Yes.

Mr. HILL. Both your personal holdings and then any in-the-money options that were in the money at the time of a filing, of an open period?

Mr. SMITH. You are referring to me?

Mr. HILL. Well, no, just your plan as a corporate officer in the plan.

Mr. SMITH. Some officers may have had a 10b5-1 plan; others may not have.

Mr. HILL. But it wasn't a requirement by the general counsel that everybody have one?

Mr. SMITH. No. The requirement was that the general counsel, as a clearing process, that he has to approve before a 16b officer can sell stock.

Mr. HILL. How many days a quarter do you think you had available for trading under those plans?

Mr. SMITH. It tends to be the first 30 days after the earnings call. We wait a day or two. Thirty-day window. The general indication is to sell it sooner in the opening versus later.

Mr. HILL. Can you think of a time when your general counsel canceled that window due to a material or nonpublic information effect while you were CEO? In other words, you couldn't use the window because people in the group had material or nonpublic information.

Mr. SMITH. There were a few times, yes.

Mr. HILL. Did you have a lead director since you were the chairman? In your public company board, did you have a lead director?

Mr. SMITH. Similar. We called it a presiding director.

Mr. HILL. Right. And when did that person find out about this?

Mr. SMITH. The 22nd of August.

Mr. HILL. OK. Thank you. My time has expired.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Minnesota, Mr. Emmer.

Mr. EMMER. Thank you, Mr. Chair.

And thank you, Mr. Smith, for sitting through this again today.

Obviously, you have heard this over and over today and in your prior three congressional hearings. I, like most people, am very concerned about the timeline of events. I appreciate the what I take is a sincere apology of yourself on behalf of Equifax and the

acknowledgement of both the human error that you point out from last March and the error in technology, the scanning process that didn't work.

But the timeline of the discovery of the issue, the sale of the company stock by three top executives, and the disclosure of the breach to the impacted American consumer, which, in Minnesota's case, I believe we have a little over 2 million that have been identified at this point, raise serious potential ethical and legal questions.

I wanted to start by echoing what our Chairman, Jeb Hensarling, said at the outset of this hearing, and that is that the company and I would say current and former executives like yourself I would hope are going to continue to cooperate to the fullest extent with the FBI, the SEC, any agency that is investigating this, so that the truth can actually get out into the light and people can know exactly what happened.

I know you can't commit on behalf of the company, but I am sure that you can commit on your own behalf, that even in your current capacity, you are going to continue to cooperate to the fullest extent.

Mr. SMITH. Absolutely.

Mr. EMMER. I wanted to talk a little bit about the area, because today it is about Equifax, but I don't know that people are talking about the—even though we all know it, it seems to be unspoken that this is such a fast-changing environment. I was in a business that will go unnamed in Minnesota, and they have this huge investment in technology. They take you into the back room, and they have got these TV screens, flat screens all around the room, and they are showing you in real time all of the attacks that are coming in by the second and the minute.

I don't think it is just about Equifax. This is a huge issue. You look, in 2014, the U.S. Postal Service had a breach that exposed personal data on almost a million employees, and they had to shut it down. The IRS, in 2015, had almost three-quarters of a million people affected by a breach. The Office of Personnel Management had one in June 2015. And even the SEC just last year had the breach of the EDGAR online filing system.

So this isn't just about Equifax; this is a much bigger issue. And in the short time that I have left, there are two areas that I would like to talk to you about. One is I get worried in this place that the snap reaction of elected officials is more regulation, more stuff that you have to comply with, which I suspect takes resources away from the stuff you are trying to do to keep up with the ever-changing technology and the way the bad guys are trying to breach these systems. I would like you to talk about that for a second before we talk about rethinking Social Security numbers and dates of birth for identification.

Mr. SMITH. Congressman, I share your views there. It is amazing. There was a recent publication that came out, I think it was last week. It talked about in 2016 alone, over 4 billion pieces of consumers' information were hacked in 1 year alone.

It is at a rate that I have not seen in my career. It is accelerating, if nothing else, and it is a real issue that I think, again, public-private partnerships can work on. If regulation can prevent a breach like this occurring again, I am all for it. This was not an

issue, in my humble opinion, that more regulation would have addressed.

Mr. EMMER. As you go forward into the next stage of your career with this experience that you now have, would you give a word of caution to those of us who are looking at this that, be very careful about if there is magic regulation because of the compliance costs that come with it and how that could negatively impact your ability or others' ability to keep up with the technology?

Mr. SMITH. Yes. I mean, oftentimes, we are all in a reactionary environment, and the first thing we think about sometimes is that regulation is the issue. I think there are a lot of things that the public-private together can do. You mentioned one of them, which is to think about the identifier that we use for the American public, and is there a solution beyond SSN.

Mr. EMMER. All right. Thank you very much.

Chairman HENSARLING. The time of the gentleman has expired. The Chair now recognizes the gentlelady from Arizona, Ms. Sinema.

Ms. SINEMA. Thank you, Mr. Chairman.

I am deeply troubled by the Equifax data breach that compromised the personal information of over 145 million Americans. Every American should take precautionary measures to ensure his or her financial security. Arizona seniors are particularly at risk and especially now. We must make sure safeguards are in place to protect them from financial fraud.

So I have been working with Congressman Bruce Poliquin of Maine to pass H.R. 3758, the Senior Safe Act. This bipartisan legislation ensures that financial institutions have the regulatory flexibility needed to report suspected instances of financial abuse of seniors.

Every Arizonan deserves to have confidence that his or her data will be kept safe when applying for a credit card, accessing a small business loan, or buying a home. And today's hearing is an important step in finding out what went wrong and what must be done to protect consumers.

Mr. Smith, thank you for being here today. By your account, it took Equifax 40 days to let the American people know via a press release about a data breach that had lasted for 77 days. Additionally, hackers exploited the failure of Equifax IT staff to patch software for the 65 days leading up to the breach. That adds up to 182 days of Equifax failing to put Arizona families first.

Your testimony before this committee seeks to detail the internal deliberations and legal consultation leading up to the press release on September 7, but it does not excuse the end result.

An Arizonan whose name, address, and Social Security number was taken on day 1 of the breach, under your watch, was left vulnerable and in the dark about the data breach for 117 days. That is disgraceful and unacceptable.

More than most, Arizonans value privacy. We value the independence to make our own financial decisions for our families and our economic futures. But instead of taking every precaution to secure our personal data, Equifax jeopardized our privacy and made millions of Arizonans significantly more vulnerable to identity theft

and financial fraud. And now we must take every step possible to minimize the damage and better address future data breaches.

It is believed that for the vast majority of Americans, this data breach was limited to their credit header data. Credit header data includes things like name, address, date of birth, known as NADOB data, as well as addresses, aliases, and Social Security numbers.

So my first question to you, Mr. Smith, is while this information alone is highly compromising, it does not include Americans' most private financial information. Are you aware of attempts by these intruders to broaden the scope of the data breach to capture private financial information? If so, were any of those attempts successful? And if not, why do you think hackers opted to forego the more private financial data?

MR. SMITH. Congresswoman, there are millions of attempted or suspicious attacks each and every year across a wide array of our data assets. We have no knowledge through the forensic audit done by Mandiant that any of the core credit, as you refer to it, data was compromised.

As to why, that goes back to the written and oral testimony I gave, which is the Apache Struts software had sat in a different environment, completely outside of the core credit file, that was not patched. That is why they were able to penetrate that environment.

MS. SINEMA. Mr. Smith, your testimony stated that it took the Equifax IT staff 76 days to notice suspicious activity after the breach began. Could you tell me exactly how were the intruders blending in with normal network traffic, while simultaneously stealing this data from Americans, and what do you think took the IT staff so long to notice the breach?

MR. SMITH. They were fairly sophisticated, they being the criminal hackers. They moved about the system without moving large—what we define, in our environment, as large files. So the files themselves in size were not suspicious.

They were also clever enough not to move at speeds—we have velocity indicators throughout the environments that would look for things that are moving at very high speeds. They were sophisticated enough to do neither.

MS. SINEMA. Thank you.

While the Equifax breach was significant, it is important to note it was still only the fifth largest data breach in the U.S., and all five of the largest data breaches have happened within the last 5 years in our country.

And we as a community here in Congress must recognize that these data breaches here are increasingly frequent, and they undermine the trust that Americans place in the marketplace and their government.

Whether it is Equifax or the Office of Personnel Management, Americans deserve to have institutions—both public and private—that work in good faith to safeguard their data from those who would harm them.

And I would urge that Congress should recognize that cybersecurity is not a niche issue to be left to the next generation.

We must find real bipartisan solutions that give Americans the opportunity to succeed.

Thank you, Mr. Chairman. I yield back my time.

Chairman HENSARLING. The gentlelady's time has expired.

The Chair now recognizes the gentleman from Ohio, Mr. Davidson.

Mr. DAVIDSON. Thank you, Mr. Chairman.

Thank you for your testimony. Thank you for your sincere apology. We recognize that all these companies are staffed by humans, and humans fail, as does technology. However, we also recognize a high duty of care responsible for a fiduciary.

I was a little concerned that I was tracking correctly the way that your reporting structure is on the board and the attention given to governance. Does IT report up through your CFO, or is that a direct report to you as the CEO?

Mr. SMITH. It is a direct report to me.

Mr. DAVIDSON. OK. Within the IT, you emphasized that you are a technology company. What is the structure like within IT? Is there an information security officer that stays in the IT channel, or is that broken out separately?

Mr. SMITH. The chief security officer, global security officer is a direct report into the general counsel of the company. The general counsel reports directly to me.

Mr. DAVIDSON. OK. So you feel that your governance structure was adequate?

Mr. SMITH. I am not sure I understand the question.

Mr. DAVIDSON. So given that this error happened, you mentioned that you had some closed-loop system failures, where you had things that are supposed to happen but you didn't have a closed-loop system to make sure they did happen. Do you feel there was any failure in governance? Was the structure part of the issue at all?

Mr. SMITH. I don't believe so. I don't think structure determines success or failure of a process or of a business. It is people and technologies doing the right thing. So having the chief security officer report into technology, report into me, report into CFO, I am not sure would change the outcome of what we just experienced.

Mr. DAVIDSON. OK. Well, that is a little concerning, but that is your philosophy.

On trading, so when you look at—aside from the cybersecurity concerns, which have been covered extensively, I was really planning to go down a similar path to my colleague, Mr. Hill, who talked about how trades for board members, executives within the company are approved, what is the timing like for that?

And I also noted that you said that there were times where because shareholders of record inside the company had information that was nonpublic and material that those trades were suspended. And I can't think of a more public time where it would probably have been appropriate to suspend a trade than while you had a breach of this. Was that an error, an omission, or do you feel that the governance worked correctly in that instance as well?

Mr. SMITH. Congressman, let me be very clear, if I may. There is a process to clear trades. It goes through the general counsel. I

am not involved in that process. These three individuals that traded, it is my understanding they had no knowledge of the breach.

You remember, back to the timeline we talked about earlier, it was the 31st was when the portal was shut down. We hired the forensic auditors and the law firm on the 2nd. It wasn't until later in mid-August that we had indication that something was going on that involved large amounts of data and PII.

These guys traded the 1st and 2nd of August. They followed the process, the protocol that we had in place at that time.

Mr. DAVIDSON. OK. So based on the knowledge that your counsel had, I assume it reviews these sorts of things, would it have been part of the procedure to say, hey, we have just had some very substantial material information that is nonpublic.

Isn't there a clear concern—4 days of testimony here, I am sure you are going to keep talking about this for a long time—that given the amount of material information that was nonpublic, that executives and board members should not be trading in these shares?

Mr. SMITH. Congressman, again, clarification: The 31st of July, the only indication we had there was a suspicious incident, no knowledge of a breach until weeks and weeks later.

Number two, it should be noted, this is a topic that is of priority for the board of directors, and there is investigation currently going on by the independent board of directors.

Mr. DAVIDSON. Do you think it was a mistake to not cancel pending trades even if they had been ordered before the discovery of this nonpublic information given that they were actually going to occur in that period?

Mr. SMITH. Congressman, on the 1st and 2nd of August we had no idea, other than a suspicious incident in a dispute portal.

Mr. DAVIDSON. Mr. Chairman, my time has expired. I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Colorado, Mr. Perlmutter. The gentleman passes at the moment.

The gentleman from Tennessee, Mr. Kustoff, is now recognized for 5 minutes.

Mr. KUSTOFF. Thank you, Mr. Chairman.

Thank you, Mr. Smith, for being here today.

If I could, Mr. Smith, I think, from my standpoint in listening to others question you today, really the most glaring problem is the length of time between when this breach occurred to when the public was notified. And I have heard your explanations this morning.

To that end, on September 7, when Equifax claimed that they recently discovered a, quote/unquote, "cybersecurity incident" involving consumer information, but, of course, you knew back in July. So if I can, let me back it up for just a moment.

From a governance standpoint, did Equifax have a pre-existing plan in place for contingency such as this, for a breach such as this?

Mr. SMITH. If I may, before I answer the question, point of clarification. I was not aware in July there was a breach. I was not aware until mid-August, as I have said before, and then not until late August that there was a breach, and even that data continued to evolve until September 7 and, again, until Monday of this week.

To answer your question specifically, Congressman, yes there was a crisis management written protocol in place, and it applied to many crises, including a data breach.

Mr. KUSTOFF. Did it anticipate a breach as big as this breach?

Mr. SMITH. No. The crisis management protocol that we have in place is a breach in general. It doesn't specify you react differently if it is 145 million versus 5 million.

Mr. KUSTOFF. Did Equifax, in fact, use that protocol for this breach?

Mr. SMITH. Yes.

Mr. KUSTOFF. Was it executed properly?

Mr. SMITH. Not without issue, as we talked about, but that is because the system, the people were overwhelmed on the sheer volume.

Mr. KUSTOFF. So I understand it, the website that you have set up to provide consumers information about the breach, which is EquifaxSecurity2017.com, in fact, that domain name was secured on or about August 22. Does that sound about right?

Mr. SMITH. That sounds about right.

Mr. KUSTOFF. All right. So that website, in some form or fashion, was ready to go some 2 weeks prior to the announcement. Is that right?

Mr. SMITH. Yes, Congressman, that is approximately right. And remember, the thing we talked about is, one, the data was still moving. It was fluid. We were wanting to be as accurate and as transparent as possible on the data; two, we talked about Mandiant, the cybersecurity forensic team had recommended that we prepare for increased cyber attacks post announcement; and third was we had to stand up the environment you are referring to so consumers can get access to free services.

Mr. KUSTOFF. I do want to follow up, at the beginning, this morning, Chairman Hensarling asked you about law enforcement. As I understand it, the FBI is involved. They are leading the investigations. Is that correct?

Mr. SMITH. That is correct.

Mr. KUSTOFF. Is the Secret Service also involved?

Mr. SMITH. Not to my knowledge.

Mr. KUSTOFF. Are there any other law enforcement agencies involved in the investigation?

Mr. SMITH. There may be. I have been so focused on the FBI.

Mr. KUSTOFF. I note that law enforcement, including the FBI, there may possibly be other law enforcement, there were other agencies that are involved in the investigation. Is there any law enforcement agency or any agency whatsoever that recommended to you or to Equifax that you not disclose this breach until when you disclosed it in September?

Mr. SMITH. To the best of my knowledge, no. They were involved starting August 2. We communicated with them routinely throughout the process. We made them aware in September. We planned on going live on September 7.

Mr. KUSTOFF. You mentioned earlier that you hired Mandiant on or around August 2. That is right?

You mentioned King & Spalding who you have hired for legal purposes. Have you also hired a PR crisis team?

Mr. SMITH. Yes, Congressman, we did.

Mr. KUSTOFF. And who is that?

Mr. SMITH. In fact, we hired two, a company called Edelman, well-known crisis management team at the tactical level to help us understand, track a variety of input from different sources, social media, broadcast media, regulators, State AGs, so on and so forth; and then a crisis management, kind of a strategic consultant as well.

Mr. KUSTOFF. You mentioned King & Spalding. Have you inquired of King & Spalding or any other law firm concerning bankruptcy protection for Equifax?

Mr. SMITH. No, sir.

Mr. KUSTOFF. No bankruptcy protection whatsoever?

Mr. SMITH. Have I consulted a law firm—

Mr. KUSTOFF. Or anyone else concerning bankruptcy protection for Equifax.

Mr. SMITH. No, sir.

Mr. KUSTOFF. Let me ask it another way: Has anybody at Equifax sought advice for bankruptcy protection for Equifax?

Mr. SMITH. Not that I am aware of.

Mr. KUSTOFF. That is all that I have. I yield back.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Maine, Mr. Poliquin.

Mr. POLIQUIN. Thank you, Mr. Chairman. Appreciate it.

Thank you, Mr. Smith, for being here. I know you have been on the Hill for quite some time, and a lot of these questions have been asked before. But this is so important because it goes central to our economy. It really does.

Here we are on a new pro-growth agenda for this country where we want to have lower taxes and fewer regulations and trade that is fair and energy prices that are lower and stable and then something like this happens.

Now, I know you folks got hacked, and I know you are doing the best you can with it. But the results of this might not be felt for quite some time. Think about this, about a third of our country, 40 percent of our country—I don't know what it is—60 percent of our adults, 145 million people, Mr. Smith, 145 million, and criminals now have the Social Security numbers, their addresses, their birth dates.

When my mom who is 89 had to go in and sign up for Medicare, what do you need? You need a Social Security number. And this is really, really serious stuff. I accept your apology. I hope the American people do. I don't know if they will. But we have a population of about 1.3 million people. I am guessing about .5 million got affected by this.

Now, I am also very concerned about the perception of wrongdoing when it comes to our securities laws. You are a publically traded company, your Equifax is. That means folks in Maine and rural Maine that I represent who are saving for college or saving for their retirement, little savers, small investors, the little guy, they can buy some of your shares in the open market and take a bet that your growth is going to reward them and take a bet on the U.S. economy.

And then all of a sudden we have material here—if you believe it. I don't know there is an investigation, I am sure, that is going on—that says that in late July you folks knew about a breach, and a breach which is central to your business. My gosh.

You folks collect all the sensitive information and you sell it to banks and automobile dealers and what have you to make sure they get accurate credit reports and money can flow through the economy and families can buy homes and get mortgages and buy cars and businesses can grow.

This is really serious stuff. So any breach of that information in your business plan is central to your success as a company and therefore it affects the stock price. So now we see information—if it is true. I don't know—that you had folks on the inside.

And it is really hard, Mr. Smith, for me to accept the fact that you had about a dozen people reporting to you and they didn't know what the heck was going on when something is so central to your business plan.

It looks like some of these folks acted—three in particular have been mentioned today—acted to sell their stock before the breach was announced, about a month before, to escape loss in the stocks that they own which is the stock in your company.

If that is the case, the little guy gets screwed. Because the guys on the inside who know this information avoid the loss, but the little folks that I represent up in Maine—and they are hardworking, and they save every penny and they are worthy of all the income they have—they have invested in your company. They have invested in America. They have invested in our economy, and they get screwed.

I have got a question for you. Now, I may be wrong about this, Mr. Smith, but the information I have that is public, it says that you own about 285,000 shares of Equifax. Is that true?

Mr. SMITH. Yes, I believe that is right.

Mr. POLIQUIN. OK. Fine. And given the—roughly, the market value of that of your outstanding price per share, it is about 28 million bucks or something. Do you or did you sell any of your stock between the time when the breach was learned on the inside and when you announced it to the public when everybody else in America had that information?

Mr. SMITH. No, sir.

Mr. POLIQUIN. OK. Here is one of the other things that drives me crazy: Confidence. We have business—out of 15-year business confidence at a 15-year high. We have consumers who are confident about the new direction for a growing economy with more jobs and fatter paychecks. And then something like this happens, which shakes our confidence.

Now, I know that Kyrsten Sinema mentioned this, and I want to support it also and ask everybody in our conference, Republicans and Democrats, to support a way for Congress to help, and that is called the Senior Safe Act.

We think it is a good idea if seniors who are very vulnerable to this sort of identity theft and fraud are able to go to their bank tellers and their insurance agents and those who plan for their retirement and say, we suspect fraud here of all types. We want to speak

up to the authorities and not be liable for doing so. That is a great bill.

Thank you, Mr. Smith, for being here. I appreciate your time.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Rothfus.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Mr. Smith, when I first heard about the breach, I was obviously very concerned, like all Americans were. Equifax, which is tasked with guarding millions of Americans' sensitive and personal data, has violated the trust of the American people. It is not acceptable, and I commend the Chairman for convening today's hearing so that we can understand what went wrong and how we can prevent it from happening in the future.

My constituents in western Pennsylvania sent me here to be their voice, so I would like to share some of their thoughts on this situation. David from Allegheny County, Pennsylvania, wrote to us, quote, "I am more than a bit angry about the Equifax data breach. While I understand that crime will always be a part of life, I am outraged by Equifax's response to the situation. They have allowed my personal information be compromised and made available. This has the potential to impact my wife and I for the rest of our lives."

Robert in Cambria County, Pennsylvania, wrote, quote, "Equifax must be held severely accountable for the massive data breach affecting nearly every adult American, including my entire family. They must answer for their weak and seemingly disingenuous initial response and notification regarding the breach."

And Alan, also from Allegheny County, described his interactions with Equifax as, quote, "an endless, circular conversation," and added, quote, "frankly, I am rather tired of this ongoing fiasco."

These are real people whose concerns need to be addressed. Hardworking Americans are scared and they deserve answers, and they need to be made whole.

I understand that—we talked about a little bit of a timeline here. Equifax discovered the breach on July 29 and notified the FBI 2 days later. Mandiant was brought in a few days after that to investigate, but Equifax did not notify the public for over a month.

I understand from your testimony that this delay was partly due to a concern that public notification would invite more bad actors to compromise your systems. With that said, it is still concerning that more than a month elapsed between discovery of the breach and public notification.

I am curious as to whether there was a specific event or fact that finally led Equifax to make the disclosure. For example, September 7 was the date that it was disclosed. Did you know something on September 7 that you did not know on September 6?

Mr. SMITH. Congressman, a point of clarification. So we did not—we were not aware of a breach of any sort back in the July time-frame you mentioned. Again, at that time it was—

Mr. ROTHFUS. Well, you noticed activity on July 29 that was suspicious?

Mr. SMITH. We notice suspicious activity on our databases around the world to the tune of millions per year. So what we saw—thought we saw in late July was nothing we haven't seen be-

fore. Suspicious activities, unfortunately, in this environment are very common.

Mr. ROTHFUS. But a couple days later you are already engaging outside vendors?

Mr. SMITH. Which that, in itself, was not unusual.

Mr. ROTHFUS. What did you know on September 7 that you did not know on September 6?

Mr. SMITH. I don't have that specific answer. I can tell you this: The timeframe between mid to late August and September 7, as I mentioned before, was very fluid. As we just saw on Monday's announcement this week, that picture continued to develop as we found 2.5 million more consumers that were impacted and announced on this Monday. So it was an ever-evolving set of facts.

Mr. ROTHFUS. You testified that the data was not encrypted on your database. Is there a reason for that?

Mr. SMITH. Again, there are different levels of security in different environments: Encryption is one, tokenization is one, masking is one, firewalls are one, encryption at rest is one, encryption in motion is another technique. So there is no one, single technique that protects the consumers' data.

Mr. ROTHFUS. A lot of people are watching at home wondering if their data was compromised in the breach. Many Americans are still wondering whether their personal information that is currently being housed at Equifax is safe. Is their information currently safe today?

Mr. SMITH. We have no knowledge that any other information we have in our database in the U.S., around the world was compromised. It was limited to this one dispute portal we have talked about now for a number of days.

Mr. ROTHFUS. Is there a reason that you are choosing not to disclose the scope of insurance coverage?

Mr. SMITH. Yes, there is.

Mr. ROTHFUS. Could you share that with us?

Mr. SMITH. I prefer not to. And the reason being, Congressman, is when you disclose a number it puts a target out there for others, for lawsuits, and so on and so forth.

Mr. ROTHFUS. That is going to be disclosed in discovery, and you already have lawsuits out there.

Mr. SMITH. Yes.

Mr. ROTHFUS. But you are choosing not to—

Mr. SMITH. Correct.

Mr. ROTHFUS. I yield back, Mr. Chairman.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from North Carolina, Mr. Budd.

Mr. BUDD. Thank you, Mr. Chairman, and Mr. Smith.

So I think what has infuriated the people I serve in North Carolina is they really didn't volunteer to have their data stored at your company. They didn't say Equifax, here, take my data. So there is an element, and it is a major one at your company, and it is a trust element, and that has really been shattered.

But let me shift over to a personnel topic. So why were the chief security officer and the chief information officer allowed to retire instead of resigning or being fired? I believe you, yourself, resigned.

Mr. SMITH. It is semantics. They are out of their job now. The day we announced they are stepping down, they are no longer effective. They are individuals who can add an advisory capacity for smooth transition between themselves and the two announced interim individuals we have at the CIO level and the chief security officer level.

And then if those individuals are replaced with full-time people, which they will be at some point in time, they can add value there. So it is nothing more than having them assist in a smooth transition.

Mr. BUDD. Beyond just semantics, what was the total cash value of their retirement packages, if you don't mind?

Mr. SMITH. I don't know specifically. We can get that information to you.

Mr. BUDD. If you would, please.

So did the chief security officer and the chief information officer undergo any financial repercussions as a result of their retirement other than foregone future salary?

Mr. SMITH. They lost their jobs, and there is no bonus.

Mr. BUDD. So just foregone future salary and no bonus, correct?

Mr. SMITH. Yes, correct. And no severance for either one.

Mr. BUDD. Did the discussion to allow them to retire instead of terminating their employment, did it increase or decrease the size and scope of their severance package with the company? You said there was no severance package.

Mr. SMITH. Correct.

Mr. BUDD. In general, does an employee at the Equifax Corporation who retires have access to more benefits, receive a better separation agreement than someone who resigns or is fired?

Mr. SMITH. Not to my knowledge.

Mr. BUDD. Well, so it is more likely than not—did Equifax not punish the individuals responsible but actually rewarded them through this decision by not firing anybody?

Mr. SMITH. No, sir. They are both out of a job.

Mr. BUDD. Chairman, I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentleman from Indiana, Mr. Messer.

Mr. MESSER. Mr. Smith, thank you for being here. You know, I admire your stamina in sitting through this, but I have to tell you, the more I hear about this, the madder I get. So excuse my tone as I go through this.

Have you had an opportunity to log onto the Equifax page and do this process of determining whether you were part of the breach?

Mr. SMITH. Absolutely.

Mr. MESSER. I did it.

Mr. SMITH. Right.

Mr. MESSER. So in that, I had to give my birth date multiple times, had to give parts or all of my Social Security number, four or five times. I answered a question or two wrong, so I had to call into the web pages—I mean call into your calling service, and I had to give my Social Security another time.

Has it crossed your mind that given the recent breach and the fact that you guys have disclosed personal information for 140 million Americans that people might be a little uncomfortable giving you their Social Security number again seven or eight times to find out whether they were impacted?

Mr. SMITH. Congressman, I have talked to a number of people myself, and I share your frustration. I share their frustration. We have tried to improve that process as much as we can, but we have to validate you are who you are before we can offer you the product.

Mr. MESSER. Well, it is frustrating to a lot of people, and obviously you haven't built a great record as an organization on trust.

Will Equifax profit from the new data now being provided by tens of millions of Americans to your website? Will Equifax be able to take that information now that I have entered it again and use it commercially for itself or for partners?

Mr. SMITH. The intent of this service is a service. It is a utility. It is to offer you this service for free, not sell, cross sell, up sell you as a consumer.

Mr. MESSER. So looking here, this is the privacy notice you have to click on when you sign onto the web page. It says here, I think, in these two columns here, that this information can be used for joint marketing with other financial companies, for affiliates, everyday business purposes, for marketing purposes by, it looks to me like Equifax and the company that is doing this for you. Is that—

Mr. SMITH. Congressman, if you are a consumer that comes in and gets a free service from us, our intent is to have that in an environment where we don't cross sell, up sell you.

Mr. MESSER. Well, the form says you will. So am I to believe you or the form?

Mr. SMITH. Excuse me?

Mr. MESSER. The form here says you will. So am I to believe you or the form?

Mr. SMITH. I am not sure what form you are referring to.

Mr. MESSER. This is the privacy notice. So, again, will Equifax have the opportunity to use the information provided by consumers in their operations of commerce, therefore make a profit on it?

Mr. SMITH. I will say it one more time. The intent is when you come to us to get a free service, we are not going to cross sell or up sell you.

Mr. MESSER. With all due respect, there is a phrase, the road to hell is paved with good intentions. I think your intentions were probably fine as 140 million people lost their information. It looks to me, based on this form, that you guys have the ability to do that.

I want to ask you this question: Have you ever met anybody who had their identity stolen, Mr. Smith?

Mr. SMITH. Yes.

Mr. MESSER. It is a pretty miserable experience, isn't it?

Mr. SMITH. Yes.

Mr. MESSER. It destroys their life. So as we talk about big numbers like 140 million people, almost 4 million people in Indiana, it is really important to remember that these people are real people that have had their lives put at risk.

Mr. SMITH. Congressman, I couldn't agree more. I have talked to people at my church that work for us, Equifax employees, people in the community, my three daughters, my wife, my family. I understand the anger and frustration they are going through.

Mr. MESSER. And I am glad you appreciate that frustration. We will return to this in just one quick second.

As we have gone through this, you have said you have these five services you are going to provide. When it comes to real compensation for people who have had their identity stolen, the reality is they are not going to get much from you. Is that fair?

Mr. SMITH. What they are going to get, Congressman, is these five free services plus the sixth service, the lock and unlock for life.

Mr. MESSER. But if their identity is stolen, the compensation for you won't be much. You said earlier you won't throw out a number. I can give you a number. Total assets of your company are about 6.6 billion based on your annual report. Is that right?

Mr. SMITH. Approximately.

Mr. MESSER. Roughly that. So if you take 147 million people, that is about \$47 per person, if you liquidate. If 1 percent of those people have some kind of damage, you have got about \$4,700 that you would have to even compensate them anyway.

I want to ask you this though, because you mentioned how frustrated you were, and I will leave you on this. This is where I think a lot of American people struggle. You would consider this a pretty major business screwup, right?

Mr. SMITH. It is a breach obviously that we are very, very sorry for.

Mr. MESSER. 147 million people.

And you mentioned—let me use your phrase—the folks that you found most directly responsible for that, they lost their job, no bonus, no severance, right? Is that what happened to the people that you held responsible for this? That is your words.

Mr. SMITH. My words are, I am ultimately responsible, and I stepped down.

Mr. MESSER. So does it seem fair to you that you would get a \$40 million to a \$90 million bonus as you exit after you presided over potentially the biggest business screwup in modern history where 140 million Americans had their personal information stolen?

Mr. SMITH. Congressman, the only thing I have walked away with is all disclosed in the proxy. It was my pension and prior compensation. I have asked for no more.

Mr. MESSER. Yes. The American people are frustrated. And again, I appreciate you being here, but they have a right to be frustrated. It doesn't seem fair.

Chairman HENSARLING. The time of the gentleman has expired.

The Chair now recognizes the gentleman from Georgia, Mr. Loudermilk.

Mr. LOUDERMILK. Thank you, Mr. Chairman.

Mr. Smith, thank you for being here. I am impressed that you are here, considering that you are no longer in your previous position. I don't know that you would have had to have been here. I appreciate your attendance here because I know this is difficult. It is a difficult time for 147 million Americans as well.

A couple questions regarding some of the things you said earlier. Where I want to be focused is how do we prevent something like this from happening again? I spent 30 years in the IT business, and security was always at the forefront of things we were working on. And so I am very interested in what transpired to cause the problem, how can we avoid this in the future.

First of all, you had mentioned in a couple of instances, as you were addressing some of the members asking questions here, that you complied with all the State laws regarding notification. And you mentioned State laws earlier regarding cybersecurity.

Is it State laws that govern our cybersecurity policy? Is there not a Federal law that governs that? And if there are, why is that not applicable?

Mr. SMITH. Congressman, the only point of clarification, the only thing we are trying to be mindful of there was as we learned and gained more insight on the size and scope and nature of the breach is making sure we balance our desire for accuracy, completeness of the picture with the State laws of communication. That is what I was referring to.

Mr. LOUDERMILK. OK. I understand. But are there Federal laws that are applicable in this instance, or is cybersecurity pretty much governed by State law?

Mr. SMITH. I am not sure what you are saying. It is not governed by State law. The State law was just the communication I was referring to.

Mr. LOUDERMILK. OK. So the actual applying of the patch, from what I understood in your previous testimony and you answering questions, was you were notified of the vulnerability. A patch was provided. It was communicated that that patch should be applied, but somewhere that did not happen. I guess, it was the human error was the individual who was to apply the patch to that portal did not follow through. Is that correct?

Mr. SMITH. It is a little bit more than that. It was an individual in the IT organization who received notification from security. That individual was responsible for the patching process and never ensured that the proper person was communicated to and did not close that loop.

Mr. LOUDERMILK. Is there a level of oversight that should be there? Quite often when I was in the military, and worked in communications and intelligence, we always had two-person integrity. There was always somebody looking over the shoulder to make sure that a process was completed.

And same thing when I was working with many governments and their IT is that especially with the security patch, that there was always someone else to come back through and make sure that it was applied. Was that process not in place?

Mr. SMITH. Yes. To clarify, this individual owned the communication and the patching process to ensure it was not closed. He did neither. Second, the closed-loop process was also the scanner we talked about. And the scanner, which is applied, I believe it was March 15, to look across the environment for this vulnerability did not find this vulnerability, and that is currently under investigation as to why.

Mr. LOUDERMILK. OK. That was—it kind of hit my next question, is that being under investigation as to why that did not happen, and is there some liability on some individuals that potentially were nefarious in this process?

Mr. SMITH. The individual who I just discussed that was responsible for the patching process is no longer with the company.

Mr. LOUDERMILK. All right. Thank you, Mr. Chairman. I yield back.

Chairman HENSARLING. The gentleman yields back.

The Chair now recognizes the gentlelady from New York, Ms. Tenney.

Ms. TENNEY. Thank you, Mr. Chairman. And thank you for having this very important meeting, as we have over 145 million U.S. consumers who have been affected by this.

And I thank you, Mr. Smith, for being here and being willing to answer these questions.

You know, everybody is really angry. Our constituents are calling us. People are concerned about the security breach. Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers for up to 200,000 consumers and all kinds of data has been breached. And it took—I know you have discussed this over and over—but 6 weeks to notify regulators.

My first question on this is, did you or your firm notify the credit bureaus before you announced this breach so they could prepare for what our consumers are trying to find answers to? And many State laws also require this. Did your company actually do that? Did you notify those credit bureaus that were your customers?

Mr. SMITH. Let me make sure I understand the question, Congresswoman. Did we notify specifically TransUnion and Experian who—

Ms. TENNEY. Right. Prior to the date that the breach was. So it took 6 weeks before the actual patch was discovered and released. That is when you got your—I don't know—I can't remember the dates on—my colleagues asked you when you got your crisis management team, when you lawyered up, when you got everybody ready before you actually disclosed that. But when did you actually notify your customers, the credit bureau customers who relied on you for your information?

Mr. SMITH. Again, I think I understand the question. So it was in late August, not late July, that the picture started to come together that we had a data security issue. We went live on September 7.

To answer your question specifically, we did not go to TransUnion or Experian before the release went out on September 7.

Ms. TENNEY. So they didn't have any knowledge of this happening, so they weren't able to prepare when this was to come later on, as your company did?

Mr. SMITH. It was not public at that time.

Ms. TENNEY. Right. Let me ask you, so you described the suspicious activity and the patches and millions of patches occur. Is there a priority or a way that your team identifies what patches are more important, more valuable, more vulnerable than others? Is there some protocol in place for that?

Mr. SMITH. Yes, there is. Let me clarify though, if I may.

Ms. TENNEY. OK.

Mr. SMITH. It is not millions and millions of patches per year. What I was referencing is, in any given year, it is not unusual to have millions of suspicious or potential attacks.

Specific to patches, patches and the requirement for patches are very common, and they are stratified in different categories, from critical to high, to medium, to low risk. And the protocol internally for the amount of time required or allowed to apply the patch depends on the criticality of the issue itself.

Ms. TENNEY. So what would you rate this patch that was what was—did not get—

Mr. SMITH. It was critical.

Ms. TENNEY. It was critical. And that didn't—when was the actual date that you discovered that patch?

Mr. SMITH. Again, March 8 we were notified by CERT of the need to patch on the 9th. The email went out to the teams to apply the patch. And as we talked about before, there was a human error. The individual did not communicate and close the process. And on the 15th of March, the scanning device did not find the vulnerability.

Ms. TENNEY. But that is in March. Did you notify the credit bureaus or the other customers? How many customers do you have on your—do you know—the confidential data is actually on your site—do you have—in control of? How many people, would you say, actual individuals are on the site that would be vulnerable, not just—

Mr. SMITH. The total credit population in the United States is roughly 230 million, 240 million people.

Ms. TENNEY. So that many people were affected by this?

Mr. SMITH. No, Congresswoman. The number we disclosed was 145.5 million. The services we are offering are to all Americans, but at this 145.5 were impacted.

Ms. TENNEY. OK. Well, let me just go quickly, because I decided to go look onto your site, as my colleague pointed out. It is ironically called TrustedIDPremier.com. And I went to this and put my own information, and it said I may have been breached.

And it does send me to another—I have to go through some protocols, re-enter more digits, my Social Security number, my name, and then it reveals to me that, nonetheless, please enter more personal information.

If people listening to this and my constituents go on to make sure—to find out if they have had their data breached, will they be vulnerable if they re-enter this on this website?

Mr. SMITH. We have taken many steps since the breach to make sure that site is very secure.

Ms. TENNEY. So this is secure? They can go re-enter their data, and it will be secure?

Mr. SMITH. Yes.

Ms. TENNEY. Thank you.

Chairman HENSARLING. The time of the gentlelady has expired.

The Chair now recognizes the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Mr. Smith, thank you for your testimony today. Thanks for lasting so long.

Just a few questions for you. And I do have some sympathy for the attack, the breach. Whether it is Anthem, BlueCross, or Lowe's, or Home Depot, or JPMorgan Chase, or personnel department, the Democratic National Committee, lots of hacks have occurred, and everybody needs to stay vigilant to that.

My questions to you, sir, are going to be more—credit reporting agencies are not everybody's best friends. You have a job where you try to actually say, this guy is a good credit risk, this gal is not a good credit risk, whatever.

And we had—and it may have been you and executives from Experian and TransUnion a few years ago, and there was a question about whether or not the algorithms that are the basis for people's credit reports were going to be disclosed to us as Members of Congress.

And I think the testimony was that those were proprietary and patentable and were key pieces of information for the different organizations. Were you one of the ones that testified for us?

Mr. SMITH. Congressman, I was not. You may be referring to the most common credit score in the industry is the score called the FICO score.

Mr. PERLMUTTER. Right.

Mr. SMITH. That may be who you are referring to.

Mr. PERLMUTTER. So we wanted to get information at that point about how a FICO score was calculated, is it fair to whoever is getting their credit score, credit report, and we were told, no, that is proprietary information. Do you know whether in this hack how you guys developed the FICO score was stolen?

Mr. SMITH. Congressman, we are a reseller, if you will, in some cases of that FICO score, and there is no indication that we housed FICO scores that were hacked in any way.

Mr. PERLMUTTER. OK. So the algorithm is that proprietary information, to your knowledge, wasn't part of this theft?

Mr. SMITH. Yes. The algorithm is developed and controlled and owned by another company called Fair Isaacs.

Mr. PERLMUTTER. And your company doesn't have how that algorithm is created or developed?

Mr. SMITH. That is correct.

Mr. PERLMUTTER. OK. I was asked by somebody from the Energy Committee, and I know you may have testified earlier today, do you know whether there was a foreign actor who was the perpetrator of this hack?

Mr. SMITH. We have engaged the FBI, and the FBI is continuing their investigation.

Mr. PERLMUTTER. There were some statements you made that there was a clever kind of ability to get around some of the safeguards you all had in terms of the speed or the volume or—

Mr. SMITH. Uh-huh.

Mr. PERLMUTTER. Is there a concern on your part or anybody at the company's part that this was an inside job?

Mr. SMITH. I have no indication of that at all.

Mr. PERLMUTTER. So, when somebody comes in and hacks, it is like they are trying to break into the bank. And your bank housed

a lot of information, if you will. And you had some safeguards. You got the patch, so there is a vulnerability that they were able to get inside the bank. But then they were able to avoid a number of the different kinds of defenses you had within the bank. Did I mishear your testimony?

Mr. SMITH. That is correct.

Mr. PERLMUTTER. So in this investigation, are you doing an internal investigation on top of the FBI investigation? How is that proceeding?

Mr. SMITH. Yes. If I understand your question, there is the forensic investigation which was done on the data that was compromised. It was done by an independent firm called Mandiant.

There is an internal investigation being done by outside counsel to look at all the processes internally and the individuals involved internally, if that answers your question. And then there is the FBI investigation as well.

Mr. PERLMUTTER. All right. Last question, just what I was looking at, there are 100 lawsuits, class-action suits, a variety of suits. You were asked by Mr. Rothfus whether you had insurance for this, are you self-insured. You didn't want to give us an amount. Do you have insurance for this?

Mr. SMITH. We have cyber insurance, yes.

Mr. PERLMUTTER. OK. And is there a self-insurance? Do you have self-insurance? Do you have money in reserve for something like this?

Mr. SMITH. There is a retention that we have and then on top of that is a stack of participants up to a limit.

Mr. PERLMUTTER. And my last question, do you still retain shares in the company?

Mr. SMITH. Absolutely.

Mr. PERLMUTTER. OK. Thank you.

Chairman HENSARLING. The time of the gentleman has expired. There are no more members in the queue.

I would like to thank the witness for his testimony today.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

I would ask Mr. Smith that you please respond as promptly as you are able. This hearing stands adjourned.

[Whereupon, at 1:44 p.m., the committee was adjourned.]

A P P E N D I X

October 5, 2017

**Prepared Testimony of Richard F. Smith
before the U.S. House Financial Services Committee**

October 5, 2017

Chairman Hensarling, Ranking Member Waters, and Honorable Members of the Committee, thank you for the opportunity to testify today.

Preliminary Statement

I am here today to recount for this body and the American people, as best I am able, what happened when Equifax was hacked by a yet unknown entity and sensitive information of over 140 million Americans was stolen from its servers, and to outline the remediation steps the company took. We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility, and I am here today to apologize to the American people myself and on behalf of the Board, the management team, and the company's employees.

Let me say clearly: As CEO I was ultimately responsible for what happened on my watch. Equifax was entrusted with Americans' private data and we let them down. To each and every person affected by this breach, I am deeply sorry that this occurred. Whether your personal identifying information was compromised, or you have had to deal with the uncertainty of determining whether or not your personal data may have been compromised, I sincerely apologize. The company failed to prevent sensitive information from falling into the hands of wrongdoers. The people affected by this are not numbers in a database. They are my friends, my family, members of my church, the members of my community, my neighbors. This breach has impacted all of them. It has impacted all of us.

I was honored to serve as the Chairman and Chief Executive Officer of Equifax for the last 12 years, until I stepped down on September 25. I will always be grateful for the opportunity to have led the company and its 10,000 employees. 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, we help millions of Americans access credit, whether to buy a house or a car, pay for college, or start a small business. During my time at Equifax, 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. Throughout my tenure as CEO of Equifax, we took data security and privacy extremely seriously, and we devoted substantial resources to it.

We now know that criminals executed a major cyberattack on Equifax, hacked into our data, and were able to access information for over 140 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.

Americans want to know how this happened and I am hopeful my testimony will help in that regard. As I will explain in greater detail below, the investigation continues, but it appears that the breach occurred because of both human error and technology failures. These mistakes – made in the same chain of security systems designed with redundancies – allowed criminals to access over 140 million Americans' data.

Upon learning 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. Equifax also recently announced an important new tool that has been under development for months that will allow consumers to lock and unlock their credit files repeatedly for life, at no cost. This puts the control of consumers' credit information where it belongs – with the consumer. We have also taken steps to better protect consumer data moving forward.

We were disappointed with the rollout of our website and call centers, which in many cases added to the frustration of American consumers. The scale of this hack was enormous and we struggled with the initial effort to meet the challenges that effective remediation posed. The company dramatically increased the number of customer service representatives at the call centers and the website has been improved to handle the large number of visitors. Still, the rollout of these resources should have been far better, and I regret that the response exacerbated rather than alleviated matters for so many.

How It Happened

First and foremost, I want to respond to the question that is on everyone's mind, which is, "How did this happen?" In my testimony, I will address both what I learned and did at key times in my role as CEO, and what I have since learned was occurring during those times, based on the company's ongoing investigation. Chronologically, the key events are as follows:

On March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") sent Equifax and many others a notice of the need to patch a particular vulnerability in certain versions of software used by other businesses. Equifax used that software, which is called "Apache Struts," in its online disputes portal, a website where consumers can dispute items on their credit report.

On March 9, Equifax disseminated the U.S. CERT notification internally by email requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. We now know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 15, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability, and the vulnerability remained in an Equifax web application much longer than it should have. I understand that Equifax's investigation into these issues is ongoing. The company knows, however, that it was this unpatched vulnerability that allowed hackers to access personal identifying information.

Based on the investigation to date, it appears that the first date the attacker(s) accessed sensitive information may have been on May 13, 2017. The company was not aware of that access at the time. Between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information, exploiting the same Apache Struts vulnerability. During that time, Equifax's security tools did not detect this illegal access.

On July 29, however, Equifax's security department observed suspicious network traffic associated with the consumer dispute website (where consumers could investigate and contest issues with their credit reports). In response, the security department investigated and immediately blocked the suspicious traffic that was identified. The department continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. The criminal hack was over, but the hard work to figure out the nature, scope, and impact of it was just beginning.

I was told about the suspicious activity the next day, on July 31, in a conversation with the Chief Information Officer. At that time, I was informed that there was evidence of suspicious activity on our dispute portal and that the portal had been taken offline to address the potential issues. I certainly did not know that personal identifying information ("PII") had been stolen, or have any indication of the scope of this attack.

On August 2, consistent with its security incident response procedures, the company: 1) retained the cybersecurity group at the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; 2) reached out, through company counsel, to engage the independent cybersecurity forensic consulting firm, Mandiant, to investigate the suspicious activity; and 3) contacted the Federal Bureau of Investigation ("FBI").

Over the next several weeks, working literally around the clock, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, how many consumers were affected, and what types of information was

accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was not; it had stopped on July 30 when the portal was taken offline). Mandiant also helped examine whether the data accessed contained personal identifying information; discover what data was exfiltrated from the company; and trace that data back to unique consumer information.

By August 11, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables.

On August 15, I was informed that it appeared likely that consumer PII had been stolen. I requested a detailed briefing to determine how the company should proceed.

On August 17, I held a senior leadership team meeting to receive the detailed briefing on the investigation. At that point, the forensic investigation had determined that there were large volumes of consumer data that had been compromised. Learning this information was deeply concerning to me, although the team needed to continue their analysis to understand the scope and specific consumers potentially affected. The company had expert forensic and legal advice, and was mindful of the FBI's need to conduct its criminal investigation.

A substantial complication was that the information stolen from Equifax had been stored in various data tables, so tracing the records back to individual consumers, given the volume of records involved, was extremely time consuming and difficult. To facilitate the forensic effort, I approved the use by the investigative team of additional computer resources that significantly reduced the time to analyze the data.

On August 22, I notified Equifax's lead member of the Board of Directors, Mark Feidler, of the data breach, as well as my direct reports who headed up our various business units. In special telephonic board meetings on August 24 and 25, the full Board of Directors was informed. We also began developing the remediation we would need to assist affected consumers, even as the investigation continued apace. From this point forward, I was updated on a daily – and sometimes hourly – basis on both the investigative progress and the notification and remediation development.

On September 1, I convened a Board meeting where we discussed the scale of the breach and what we had learned so far, noting that the company was continuing to investigate. We also discussed our efforts to develop a notification and remediation program that would help consumers deal with the potential results of the incident. A mounting concern also was that when any notification is made, the experts informed us that we had to prepare our network for exponentially more attacks after the notification, because a notification would provoke "copycat" attempts and other criminal activity.

By September 4, the investigative team had created a list of approximately 143 million consumers whose personal information we believed had been stolen, and we continued our planning for a public announcement of a breach of that magnitude, which included a rollout of a

comprehensive support package for consumers. The team continued its work on a dedicated website, www.equifaxsecurity2017.com, where consumers could learn whether they were impacted and find out more information, a dedicated call center to assist consumers with questions, and a free credit file monitoring and identity theft protection package for all U.S. consumers, regardless of whether they were impacted.

I understand that Equifax kept the FBI informed of the progress and significant developments in our investigation, and felt it was important to notify the FBI before moving forward with any public announcement. We notified the FBI in advance of the impending notification.

On September 7, 2017, Equifax publicly announced the breach through a nationwide press release. The release indicated that the breach impacted personal information relating to 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.

These are the key facts as I understand them. I also understand that the FBI's investigation and Equifax's own review and remediation are ongoing, as are, of course, numerous other investigations.

Protecting U.S. Consumers Affected by the Breach

From the third week in August, when it became clear that our worst fears had come true and Equifax had experienced a significant breach, my direction was to continue investigating but first and foremost to develop remediation to protect consumers from being harmed and comply with all applicable notification requirements, based on advice of outside cybersecurity counsel and Mandiant. Significantly, a major task was the need to deploy additional security measures across the entire network because we were advised that as soon as Equifax announced the hack, there would be a dramatic increase in attempted hacking. There were three main components to Equifax's plan: 1) a website where consumers could look up if they were affected by the breach and then register for a suite of protective tools; 2) a call center to answer questions and assist with registration; 3) the package of tools themselves that the company was offering to everyone in the country. The task was massive – Equifax was preparing to explain and offer services to every American consumer.

First, a new website was developed to provide consumers with additional information – beyond the press release – about the nature, extent, and causes of the breach. This was extremely challenging given that the company needed to build a new capability to interface with tens of millions of consumers, and to do so in less than two weeks. That challenge proved overwhelming, and, regrettably, mistakes were made. For example, terms and conditions attached to the free solutions that Equifax offered included a mandatory arbitration clause. That provision – which was never intended to apply in the first place – was immediately removed as soon as it was discovered. (I was informed later that it had simply been inadvertently included in terms and conditions that were essentially “cut and pasted” from a different Equifax offering.)

The initial rollout of Equifax's call centers had frustrating shortcomings as well. Put simply, the call centers were confronted by an overwhelming volume of callers. Before the breach, Equifax had approximately 500 customer service representatives dedicated to consumers, so the company needed to hire and train thousands more, again in less than two weeks. To make matters worse, two of the larger call centers in Florida were forced to close for a period of time in the wake of Hurricane Irma. The closure of these call centers led to a reduction in the number of available customer service representatives and added to the already significant wait times that callers experienced. Many needlessly waited on hold or were otherwise unable to have their questions answered through the call centers, which I deeply regret. My understanding is that the call centers are now fully functional. The number of customer service representatives, which is now over 2,500, continues to increase, and I am informed that wait times have decreased substantially.

Beyond the website and the call centers, the company also developed a comprehensive support package for all American consumers, regardless of whether they were directly affected by the incident or not, that includes free: 1) credit file monitoring by all three credit bureaus; 2) Equifax credit lock; 3) Equifax credit reports; 4) identity theft insurance; and 5) Social Security Number "dark web" scanning for one year. Importantly, enrolling in the program is free, and will not require consumers to waive any rights to take legal action for claims related to the free services offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.

Despite these challenges, it appears that Equifax's efforts are reaching many people. As of late September, the website had received over 420 million hits. And similarly, as of late September, over 7.5 million activation emails have been sent to consumers who registered for the program.

Equifax also recently 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. 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.

The hard work of regaining the trust of the American people that was developed over the course of the company's 118 year 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.

How to Protect Consumer Data Going Forward

It is extremely important that notwithstanding the constant threat of cybercriminals, the American people and the Members of this Committee know that Equifax is doing everything in its power to prevent a breach like this from ever happening again. Since the potential breach was discovered, those inside and outside the company have worked around-the-clock to enhance the Company's security measures. While I am limited in what I can say publicly about these specific

measures, and going forward these questions are best directed to new management, I want to highlight a few steps that Equifax has already taken to better protect consumer data moving forward, including the website developed to respond to the hack, and some changes still to come.

In recent weeks, vulnerability scanning and patch management processes and procedures were enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken in recent weeks to shore up its security protocols.

Importantly, Equifax's forensic consultants have recommended a series of improvements that are being installed over the next 30, 60, and 90 day periods, which the company was in the process of implementing at the time of my retirement. In addition, at my direction a well-known, independent expert consulting firm (in addition to and different from Mandiant) has been retained to perform a top-to-bottom assessment of the company's information security systems.

Beyond the recent technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company. Accountability starts at the top and I, therefore, decided to step down as CEO and retire early to allow the company to move forward. Before I retired, our Chief Information Officer and Chief Security Officer also left the company. Equifax's interim appointments for each of these positions, including Paulino do Rego Barros, Jr., the interim CEO, are ready, able and qualified to step into their new roles and to help consumers, and the company, recover from this regrettable incident.

It is my hope and expectation that, at the conclusion of the investigation, we will have an even more complete account of what happened, how future attacks by criminal hackers can be deterred and suspicious activity curbed more quickly, and most importantly, how consumers' concerns about the security of their personal data can be alleviated.

Toward a New Paradigm in Data Security

Where do we go from here? Although I have had little time for reflection regarding the awful events of the last few weeks, this humbling experience has crystalized for me two observations: 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. To my profound disappointment, Equifax now finds itself on that list. I have stepped away from a company I have led and loved and help build for more than a decade. But I am not stepping away from this problem and I am strongly committed to helping address the important questions this episode has raised. Part of that starts today, as I appear at this hearing and others voluntarily to share what I know. Going forward, however, 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.

Conclusion

Chairman Hensarling, Ranking Member Waters, and Honorable Members of the Committee, thank you again for inviting me to speak with you today. I will close by saying again how so sorry I am that this data breach occurred. On a personal note, I want to thank the many hard-working and dedicated people who worked with me for the last 12 years, and especially over the last eight weeks, as we struggled to understand what had gone wrong and to make it right. This has been a devastating experience for the men and women of Equifax. But I know that under the leadership of Paulino and Mark they will work tirelessly, as we have in the past two months, to making things right.

I realize that what I can report today will not answer all of your questions and concerns, but I can assure you and the American public that I will do my level best to assist you in getting the information you need to understand this incident and to protect American consumers.

ConsumersUnion

POLICY & ACTION FROM CONSUMER REPORTS

October 2, 2017

United States House of Representatives
Washington, D.C. 20515

Dear Representative,

Consumers Union, the policy and mobilization division of Consumer Reports,¹ writes to urge Congress to take long overdue action to protect the sensitive personal information of Americans. Last month, Equifax announced a monumental data breach affecting 143 million individuals. The breach exposed highly sensitive personal data—including Social Security numbers, driver's license numbers, and birth dates—and exploited a vulnerability that had been publicly announced several months earlier.² As a result of this breach, nearly half of the U.S. population is at risk of identity theft, potentially for the rest of their lives. Over 200,000 people have signed our petition asking Congress to take decisive action to hold Equifax accountable, and to provide stronger protections over their personal information.³

Although this is one of the largest breaches to date, it is hardly the first to put consumers' data at risk. Over the last 15 years, hundreds of companies ranging from high-end retailers to hotel chains, and from pharmacies to data brokers, have been compromised, with consumers bearing the brunt of the harm. And while breaches can occur even when companies take reasonable precautions, many breaches have been caused by companies' carelessness and lack of accountability. After years of failed bills and stalled debates, it is time for Congress to make data security a national priority, and to pass a law establishing these essential consumer protections:

- **Strong data security and data breach notification requirements for companies;**
- **Free security freezes, and better access to fraud alerts for consumers;**
- **Stronger controls over the sensitive data that credit bureaus collect and use.**

¹ Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of financial services, privacy and data security, auto and product safety, healthcare, and food safety, among many other areas. Using its more than 60 labs, auto test center, and survey research center, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

² *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX.COM (Sept. 15, 2017), <https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/>.

³ *Congress Must Hold Equifax Accountable*, CONSUMERS UNION (Sept. 8, 2017), https://secure.consumersunion.org/site/SPageNavigator/20170908EquifaxPetitionPage.html;jsessionid=00000000.ap2223b?NONCE_TOKEN=9918995BF13130F7A53497A05E2E6FAC (last visited Sept. 28, 2017).

The failure to protect personal data causes real harm to consumers. Over 15 million U.S. consumers fell victim to identity theft in 2016, costing them \$16 billion.⁴ Victims spend precious time and money repairing the damage to their credit and accounts. Medical identity theft, in which thieves use personal information to obtain medical services, exhausts consumers' insurance benefits and leaves them with exorbitant bills. Tax identity theft occurs when thieves use consumers' Social Security numbers to obtain tax refunds. Fraudulent information on credit reports also causes consumers to pay more for a loan or be denied credit. And breaches take a toll on businesses too—in 2017, the average cost of a breach to companies globally was \$3.62 million.⁵ But despite these clear harms, little has been done at the federal level to ensure that companies protect sensitive consumer data. As a result, hackers continue to target vulnerable companies—year in and year out, and increasingly from overseas.

Without a clear regulatory framework for data security, Equifax and other companies across the marketplace have insufficient incentives to be better stewards of consumers' personal data. The market simply will not fix this problem—indeed, it was not until the states began enacting data breach laws in the early 2000s that companies even disclosed their breaches to the public. Although virtually all of the states have now passed these laws, few have *data security* laws, which are needed to prevent breaches from happening in the first place. And while the Federal Trade Commission (FTC) has taken many dozens of actions against companies that fail to protect consumer data, there are many gaps in its enforcement authority that put consumers at risk. In addition, even as many companies profit handsomely from using consumer data, they offer consumers little or no control over their data practices, and little or no recourse for data lapses.

Equifax is a prime example. Consumers have no say in whether their data is shared with Equifax, even though the company makes hundreds of millions in profits from consumer data every year.⁶ Further, its reckless handling of the breach and its aftermath—including its delay in addressing a known vulnerability, delay in providing breach notices, meager remedies for consumers, inclusion of a forced arbitration provision, and rollout of a defective website—suggest that consumers rank very low on the company's list of priorities.⁷ On September 14, Consumers Union wrote a letter to Equifax laying out seven steps it must take to make consumers whole: (1) free credit freezes at all the major credit bureaus; (2) free credit monitoring

⁴ *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN (Feb. 1, 2017), <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>.

⁵ *Cost of Data Breach Study*, IBM (2017), available at <https://www.ibm.com/security/data-breach/index.html>.

⁶ Equifax, Inc., Annual Report (Form 10-K), at 27 (Jan. 31, 2017), available at <https://www.sec.gov/Archives/edgar/data/33185/000003318517000008/efx10k20161231.htm#sA091C585A07E5A24BBC2E110B9762C1A> (\$489 million in net income in 2016).

⁷ While CEO Richard Smith was forced to step down after the breach, his \$90 million severance package is unlikely to deter other executives from similar behavior. Jen Wiczner, *Equifax CEO Richard Smith Who Oversaw Breach to Collect \$90 Million*, FORTUNE (Sept. 26, 2017), <http://fortune.com/2017/09/26/equifax-ceo-richard-smith-net-worth/>.

indefinitely; (3) more detail about the security incident; (4) no mandatory arbitration clauses; (5) sufficient staff to review and process disputes; (6) a fund to compensate injured consumers; and (7) an investigation of the three officials who sold stock just prior to the breach's announcement.⁸ To date, Equifax's response to these requests has been negligible. It is time for Congress to protect consumers and give them greater control over their personal data.

Strong data security requirements, with tough penalties for violations.

First and foremost, Congress should require companies to implement reasonable data security procedures to protect consumer information. For years, Congress has failed to establish baseline requirements for data security, and consumers have paid the price. Although there are laws currently on the books, they contain many gaps and impose few if any sanctions for noncompliance. Notably, the Gramm-Leach-Bliley Act requires reasonable data security for financial institutions, but does not apply to other types of companies or provide fines for violations.⁹ The Fair Credit Reporting Act (FCRA) similarly requires credit bureaus to implement reasonable procedures to protect data, but is limited to that one industry and only applies to some of the databases the credit bureaus maintain.¹⁰

Outside these specific industries, the federal legal protections are even weaker. The FTC has used its general purpose consumer protection authority to take action against over 60 companies with lax data security practices.¹¹ However, the FTC lacks authority over banks, common carriers, and nonprofit entities, and generally cannot impose fines for violations.¹²

For example, in the FTC's cases against TJX, Reed Elsevier, and Uber, there were no fines or other financial sanctions.¹³ Additionally, earlier this year, the FTC brought an action against D-Link, a company that manufactures webcams designed for the very purpose of helping consumers monitor and secure their homes. Despite the fact that there were several known security weaknesses in D-Link's security systems, making them vulnerable to takeover by malicious software, a judge ruled that to substantiate some of the charges, the FTC needed to

⁸ Octavio Blanco, *Consumers Union Demands Equifax Make Affected Consumers Whole*, CONSUMER REPORTS (Sept. 14, 2017), <https://www.consumerreports.org/equifax/consumers-union-demands-equifax-make-affected-consumers-whole/>.

⁹ Pub. L. No. 106-102, 113 Stat. 1338 (1999).

¹⁰ 15 U.S.C. § 1681. Equifax has said that its breach only affected certain databases, calling into question whether the FCRA applies.

¹¹ See Fed. Trade Comm'n, Data Security, <https://www.ftc.gov/datasetsecurity>.

¹² In addition, few states have passed data security, as opposed to data breach, laws.

¹³ *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data*, FED. TRADE COMM'N (Mar. 27, 2008), <https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx>; *Uber Settles FTC Allegation that It Made Deceptive Privacy and Data Security Claims*, FED. TRADE COMM'N (Aug. 15, 2017), <https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data>.

show that consumers had been harmed, not just that D-Link's actions put consumers at risk.¹⁴ However, in the event of a data breach, it is often difficult, if not impossible, to reliably attribute harm to a particular incident. Hackers do not typically disclose the source of the information they use to defraud consumers, and may wait for years to use it. And consumers who are harmed often have no way to trace the harm back to a particular company, or to a particular breach that may or may not have been announced.

Congress must address these problems by establishing strong federal data security requirements with tough civil penalties. The law should cover not just financial data but any information that, if breached, could put consumers at risk. Congress should also empower the FTC to develop rules to implement these requirements, in order to give greater clarity to companies covered by the law, and allow for updated standards as threats evolve. And to ensure sufficient and appropriate enforcement, state attorneys general should be able to enforce the new law, and there should be a private right of action, with a ban on mandatory arbitration provisions.

As part of the new law, Congress should include provisions to limit the harms caused by the overuse of Social Security numbers (SSNs). SSNs are too frequently compromised in high-profile incidents, such as the recent Equifax and Office of Personnel Management breaches. Overuse of SSNs in consumer transactions creates increased risk, and invites further attempted breaches. A number of states, including California and New York, have already passed laws that prohibit public display of SSNs, including on ID cards, but Congress should extend these protections to every state.¹⁵

Similarly, all consumers should have the ability to protect their SSNs when doing their taxes. In 2016, the IRS intercepted nearly 1 million fraudulent tax returns, totaling \$6.5 billion.¹⁶ Disclosure of SSNs leaves consumers vulnerable to criminals who choose to submit a false tax return in the consumer's name and steal their tax refund. Only consumers in Florida, Georgia, and the District of Columbia, and those who are invited to do so by the IRS, may request an IRS Identity Protection PIN, a six-digit number used to confirm the consumer's identity, to help protect against this type of fraud.¹⁷ Congress should ensure that all consumers have the ability to do so.

¹⁴ *FTC v. D-Link Systems, Inc.*, No. 3:17-cv-00039-JD at 8-9 (N.D. Cal. Sept. 19, 2017) (order re: motion to dismiss), available at <https://consumermediallc.files.wordpress.com/2017/09/dlinkdismissal.pdf>.

¹⁵ Consumers Union and the State Public Interest Groups, *The Clean Credit and Identity Protection Act: Model State Law*, 1-3 (Jan 2011), available at <http://consumersunion.org/pdf/model.pdf>.

¹⁶ Written Testimony of John A. Koskinen Before the Senate Finance Committee on the 2017 Filing Season and IRS Operations, INTERNAL REVENUE SERV. (Apr. 6, 2017), available at <https://www.irs.gov/newsroom/written-testimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operations-april-6-2017>.

¹⁷ Internal Revenue Serv., *The Identity Protection PIN (IP PIN)*, (Oct. 1, 2017), <https://www.irs.gov/identity-theft-fraud-scams/the-identity-protection-pin-ip-pin>.

Strong data breach notification law, as a federal floor for consumer protections.

Congress should also pass a federal data breach law to ensure that all consumers receive notice in the event of a breach. Although data breach laws have been adopted in all but two states, these laws are inconsistent, and some offer insufficient protections. For example, many state laws have high thresholds for notice to consumers, or fail to define personal information broadly enough.

Consumers Union has a long history of advocating for strong data breach notification laws, including the first in the nation—California’s, passed in 2002.¹⁸ The premise of these laws is that an entity that has experienced a security breach should not get to decide whether or not to notify consumers about it. For consumers, notice of a data breach is necessary so that they can protect themselves from identity theft or other harms. These laws also provide incentives for companies and government agencies to take data protection seriously.

The new federal law should provide a consistent, minimum obligation to notify consumers if their sensitive personal information has been breached. This basic obligation should not preempt the states, which have led the nation’s efforts on data breach notification, from passing or enforcing stronger laws to protect consumers. Indeed, if a federal law were to preempt more protective state laws, the new law would have the perverse effect of weakening the already too weak incentives for companies to safeguard personal data. Unfortunately, many of the data breach bills proposed in recent Congresses do just that.

As noted above, a strong federal bill must cover all information that can be used to harm consumers and authorize civil penalties adequate for deterrence. Further, it should give the FTC rulemaking authority, authorize enforcement by the state attorneys general, and grant private rights of action, with no mandatory arbitration.

Free access to security freezes and better access to fraud alerts for consumers.

All 50 states and the District of Columbia now have laws on the books that permit consumers to place a security freeze on their credit reports with the major credit bureaus. Consumers Union played a key role in supporting the first one, enacted in California in 2001.¹⁹ A security freeze gives consumers the choice to “freeze” or block access to their credit file against anyone trying to open up a new account or get new credit in their name.

As with data breach notification laws, the protections of the state security freeze laws vary. Not all states allow parents or guardians to place security freezes on a minor’s credit reports, and most states allow credit bureaus to charge fees to place or lift a freeze. Moreover, no states that we are aware of provide consumers the right to place a freeze on their specialty

¹⁸ See http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.

¹⁹ See https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200120020SB168.

consumer reports. Specialty consumer reports contain information on consumer's medical conditions, drug prescriptions, tenant history, employment, check writing, and insurance claims.

Consumers also face barriers in setting up fraud alerts. When a fraud alert has been included in a consumer's credit file, potential creditors must take an extra step to confirm the consumer's identity before extending credit. While fraud alerts are not as strong as security freezes, it should be easier for consumers to take advantage of that option if they choose. Under the FCRA, initial fraud alerts last a minimum of 90 days, at which point they may be renewed by the consumer. In addition, those requesting the alert must claim that they suspect that they are—or are about to be—a victim of fraud, such as identity theft.²⁰

To address these problems, Congress should pass legislation that gives consumers easier access to security freezes and fraud alerts. Ideally, a federal security freeze law should:

- Ensure that consumers may not be charged for any security freeze services;
- Provide consumers an additional free credit report and a free credit score when placing a security freeze;
- Allow consumers to place freezes not only on reports and scores from credit reporting agencies but also on specialty consumer reports;
- Allow parents or guardians to place freezes on minors' reports;
- Clarify that all consumers may request an initial fraud alert, and extend the minimum period for an initial fraud alert for at least one year; and
- Authorize meaningful penalties for violations.

Stronger controls over the sensitive data that credit bureaus collect and use.

The Equifax breach illustrates the enormous range of information that credit bureaus collect about consumers—information that determines whether consumers get jobs, loans, insurance, phone service, cars, and many other services that are essential to daily life. To ensure that consumers are not denied these benefits based on flawed information, Congress should strengthen existing requirements governing credit report accuracy and fairness.

In particular, Congress should direct the Consumer Financial Protection Bureau (CFPB) to issue rules with more specific requirements for the credit bureaus and data furnishers, to make it easier for consumers to correct credit reporting errors. According to the FTC, about one in five consumers has a confirmed error on one or more of their reports from a major credit bureau.²¹ Credit reporting is the third most-complained about topic to the CFPB, and over three-quarters of

²⁰ 15 U.S.C. § 1681c-1(a)(1).

²¹ *In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports that Could Result in Less Favorable Terms for Loans*, FED. TRADE COMM'N (Feb. 11, 2013), <https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports>.

those complaints are related to errors on a consumer's credit report.²² Today, too many consumers suffer from errors and inaccuracies on their credit reports—many of them because they are victims of identity theft. The average victim of identity theft spends far too much time—an average of seven hours, but the process can sometimes take six months or more—addressing the resulting financial and credit problems.²³

Persistent problems with the credit reporting process include “mixed files”—when another consumer's data is mistakenly in the credit file—and failure to thoroughly investigate an error dispute. Too often, credit bureaus simply pass error disputes on to furnishers, who may reconfirm existing information in their databases without conducting a thorough review.²⁴ Therefore, we recommend that Congress impose new accuracy requirements on credit bureaus, such as matching requirements to ensure the right information is assigned to the right file. Congress should also require credit bureaus to forward to the furnisher—and require furnishers to thoroughly examine—all documentation provided by the consumer in the event of a dispute.²⁵

The credit reporting industry should also make it easier for consumers to access their own credit files and scores. Consumers are guaranteed a free credit report once a year from each of the three major credit bureaus. However, given the risks of identity theft that consumers now face, Congress should ensure that all consumers have access to more than one free credit report each year, and that specialty consumer reporting agencies are also required to provide free reports at no charge every year. Likewise, all consumers should be guaranteed access, for free, to a reliable credit score that is used by lenders when they access their free credit reports.

Finally, Congress should consider barring credit bureaus and lenders from using certain data elements in the credit decision process due to significant concerns about disparate impact, transparency, privacy, and the predictive value of that data.²⁶ For example, credit bureaus and lenders should not be permitted to use social media and web browsing data in deciding whether to grant credit. Not only could this reinforce inequalities in credit scoring along lines of race and ethnicity, but it is unclear whether the data is predictive of a consumer's ability to repay.²⁷ Moreover, the chilling effect on free expression and free association is too great—consumers

²² Consumer Fin. Prot. Bureau, Monthly Complaint Report, 5, 12 (Feb. 2017), *available at* https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201702_cfpb_Monthly-Complaint-Report.pdf.

²³ U.S. Dep't of Justice, Victims of Identity Theft, 2014 10 (Sept. 2015), *available at* <https://www.bjs.gov/content/pub/pdf/vit14.pdf>.

²⁴ Consumer Fin. Prot. Bureau, Supervisory Highlights Consumer Reporting Special Edition, 10-11, 20-21 (Mar. 2017), *available at* http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

²⁵ See Maureen Mahoney, *Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers*, CONSUMERS UNION (Apr. 9, 2014), <http://consumersunion.org/wp-content/uploads/2014/04/Errors-and-Gotchas-report.pdf>.

²⁶ See *Big Data: A Big Disappointment for Scoring Consumer Risk*, NAT'L CONSUMER LAW CTR. (Mar. 2014), *available at* <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

²⁷ Robinson + Yu, *Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace* 21-22 (Oct. 2014), https://www.teamupturn.com/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf.

should not be worried that the websites they browse and the people they connect with on social media will be used to determine their creditworthiness.

Conclusion

For too long, inadequate federal laws have allowed companies to collect and profit from the use of consumers' personal information, without consumers' knowledge or control, and without the incentives to properly steward that information and protect it from criminals. Given the unprecedented level of data collection in today's marketplace, and emergence of new privacy threats every day, now is the time to ensure that all Americans have the data protections they deserve. Consumers Union looks forward to working with members of Congress, in a bipartisan fashion, to address these vital consumer protection issues.

Sincerely,

Jessica Rich
Vice President, Policy and Mobilization

Justin Brookman, Director, Consumer
Privacy and Technology Policy

Anna Laitin, Director, Financial Policy

Consumers Union
1101 17th Street, NW, Suite 500
Washington, DC 20036

CAROLYN B. MALONEY
12TH DISTRICT, NEW YORK
2308 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3212
(202) 225-7944
COMMITTEES:
FINANCIAL SERVICES
GOVERNMENT REFORM
JOINT ECONOMIC COMMITTEE,
[SENIOR HOUSE DEMOCRAT]



Congress of the United States
House of Representatives
Washington, DC 20515-3212

DISTRICT OFFICES:
☐ 1654 THIRD AVENUE
SUITE 311
NEW YORK, NY 10128
(212) 860-0606
☐ 31-19 NEWTOWN AVENUE
ASTORIA, NY 11102
(718) 932-1804
☐ 618 LORIMER STREET
BROOKLYN, NY 11211
(718) 349-5972
WEBSITE: www.house.gov/maloney

September 13, 2017

Mr. James M. Peck
Chief Executive Officer
TransUnion
555 West Adams Street
Chicago, IL 60661

Mr. Brian Cassin
Chief Executive Officer
Experian
475 Anton Boulevard
Costa Mesa, CA 92626

Dear Mr. Peck and Mr. Cassin:

I am writing with regard to the recent data breach at Equifax, which is one of the largest, most devastating data breaches in history. The Equifax breach has affected roughly 143 million American consumers, and because of the nature of the information that was stolen — largely Social Security numbers and birth dates, which are both critical and unchangeable for consumers — criminals could be using this information to steal consumers' identity for years to come.

According to press reports, hackers in the Equifax case exploited a flaw in the open-source server software Struts, created by the Apache Foundation, to gain access to the consumers' confidential information.¹ The Struts software is widely used by large companies — by one estimate, 65% of Fortune 100 companies use Struts² — and TransUnion has publicly acknowledged that it also uses Struts.³ Despite the fact that Apache released patches for security flaws in the Struts software in March,⁴ Equifax reportedly had not applied these patches.⁵

Accordingly, I respectfully request answers from each of you to the following questions:

1. What steps, if any, has your company taken in response to the Equifax data breach? Has your company undertaken a review of your information security program to identify potential weaknesses in light of the Equifax data breach?
2. Does your company use the Apache Struts software for any of its databases? If so, do these databases contain sensitive or personally identifiable information about consumers?

¹ See, Kevin Dugan, "Equifax Blames Giant Breach on Vendor Software Flaw," *New York Post* (September 8, 2017); see also Teri Robinson, "Apache Struts Vulnerability Likely Behind Equifax Breach, Congress Launches Probes," *SC Media* (September 12, 2017).

² *Id.*

³ Laura Alix, "Panic Over Equifax Breach Bleeds to TransUnion," *American Banker* (September 12, 2017).

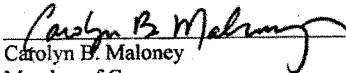
⁴ Dan Goodin, "Critical Vulnerability Under 'Massive' Attack Imperils High-Impact Sites," *Ars Technica* (March 9, 2017).

⁵ Dustin Volz and David Shepardson, "Criticism of Equifax Data Breach Response Mounts, Shares Tumble," *Reuters* (September 8, 2017).

3. Has your company applied all of the necessary security patches that Apache has released for the Struts software?
4. Are you aware of any evidence that hackers have compromised your company's information security and stolen sensitive or personally identifiable information about consumers?

If you have any questions about this request, please contact my office at (202) 225-7944.

Sincerely,


Carolyn B. Maloney
Member of Congress



Experian
900 17th Street NW, Suite 1050
Washington, DC 20006
202 682 4613 T

October 2, 2017

The Honorable Carolyn B. Maloney
U.S. House of Representatives
2308 Rayburn House Office Building
Washington, DC 20515

Dear Congresswoman Maloney,

I am responding to your September 13 letter on behalf of Experian CEO Brian Cassin. The Equifax breach is an unprecedented incident and we are still learning about what happened. We appreciate your interest in learning about Experian's response to the Equifax breach, and I want to respond to each of your questions.

As preface, and as you know, credit reporting agencies are obligated to meet the same information security standard as banks and other financial institutions. Our obligations are defined by the FTC Safeguards rule pursuant to the Gramm-Leach-Bliley Act.

1. **What steps, if any, has your company taken in response to the Equifax data breach. Has your company undertaken a review of your information security program to identify potential weaknesses in light of the Equifax data breach?**

Upon learning about the breach at Equifax, we immediately put all of our information security resources on high alert. We reviewed historical and current data to ensure that our systems were not impacted as a result of the same vulnerability, which they were not. We scanned our infrastructure to ensure no artifacts related to the activities which occurred at Equifax were present in our environment, which they were not. We reviewed critical systems to verify their continued integrity and security. We accelerated on-going projects which will enhance protections relevant to the recent event. These efforts are consistent with the extensive work we have undertaken through a sustained, year-over-year investment in our security program to ensure it is developing at pace with evolving threats.

2. **Does your company use the Apache Struts software for any of its databases? If so, do these databases contain sensitive or personally-identifiable information about consumers?**

The Apache Struts software is widely used by the vast majority of commercial and government enterprises that have Website interfaces. Experian is no exception, even though we have been migrating to newer software technologies and plan to continue this migration. Where we use Apache Struts software in connection with sensitive or personally-identifiable information about consumers, we continuously review and patch or remediate any vulnerabilities as necessary, following financial industry standard patching routines.

3. **Has your company applied all of the necessary security patches that Apache has released for the Struts software?**

Experian's data security program includes special provisions, policies and procedures for patching all software systems we use, including the Apache Struts vulnerability referenced by Equifax, CVE-2017-5638. We applied the patch to this vulnerability in our system in a timely manner. Following this remediation, Experian was no longer exposed to that vulnerability. In addition, Experian has invested in web application firewalls (WAFS) to provide another line of defence so that intrusions can be stopped at the firewall. All WAFS receive automatic updates as soon as a vulnerability countermeasure is released.

4. Are you aware of any evidence that hackers have compromised your company's information security and stolen sensitive or personally-identifiable information about consumers?

A key component of our security is continuous, robust monitoring of all systems, including, for example, monitoring of traffic and processing volumes, in order to detect any anomalies and trigger alerts, which require immediate action. Based upon our current monitoring program, as well as the steps we took as outlined in Question 1, we are confident that our systems containing sensitive personally identifiable information have not been compromised. Nonetheless, we have elevated our monitoring systems and protocol since the Equifax breach was announced.

Beyond the data security aspects of the Equifax breach, Experian also took immediate action to accelerate our consumer response capability once we became aware of the breach, which was at the same time as the general public. We put our call centers on alert, approved overtime allocations, and acquired additional technology to better respond to the volume of consumer inquiries we were receiving through our call centers and website.

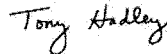
We updated our website, www.experian.com, by placing a link that directed consumers with questions about the breach to an assistance page that describes the various options consumers have to protect themselves from identity theft. We have also published FAQs that answer the most common questions about what actions consumers can consider taking, including contacting the FTC and the CFPB for additional information.

We began monitoring and engaging consumers through social media to help direct them to the right resources related to identity protection. We also are working with journalists and the media to provide information that consumers can use to understand the potential risks they may face following a data breach, including education about the differences between an initial fraud alert and a credit freeze. The activity on our phone lines and websites has been dramatically higher since the news broke, but we are prepared to so support consumers who are contacting us with concerns.

My colleagues at Experian and I wish to be of continued assistance to you as Congress continues its investigation of the Equifax breach. I would be happy to arrange a briefing for you and your staff with our Chief Information Security Officer at your request.

Thank you for contacting us with your questions.

Sincerely,



Tony Hadley
Senior Vice President
Government Affairs and Public Policy

Privacy Notice

FACTS

WHAT DOES TrustedID, Inc. DO WITH YOUR PERSONAL INFORMATION?

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and credit card information
- Payment history and transaction history
- Credit scores and credit history

All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons TrustedID, Inc. chooses to share; and whether you can limit this sharing.

| Reasons we can share your personal information | Does TrustedID, Inc. share? | Can you limit this sharing? |
|--|-----------------------------|-----------------------------|
| For our everyday business purposes—such as to process your transactions; maintain your account(s); respond to court orders and legal investigations; or report to credit bureaus | YES | NO |
| For our marketing purposes—to offer our products and services to you | YES | NO |
| For joint marketing with other financial companies | YES | NO |
| For our affiliates' everyday business purposes—information about your transactions and experiences | YES | NO |
| For our affiliates' everyday business purposes—information about your creditworthiness | NO | We do not share. |
| For our affiliates to market to you | NO | We do not share. |
| For nonaffiliates to market to you | NO | We do not share. |

JEB HENSARLING, TX, CHAIRMAN

United States House of Representatives
Committee on Financial Services
Washington, D.C. 20515

MAXINE WATERS, CA, RANKING
MEMBER

October 4, 2017

The Honorable Jeb Hensarling
Chairman
Committee on Financial Services
United States House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

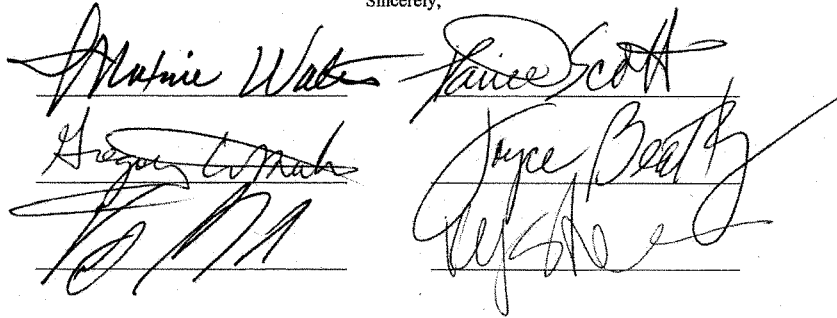
Dear Chairman Hensarling:

In accordance with Clause 2(j)(1) of Rule XI of the Rules of the House, and Clause (d)(5) of Rule 3 of the Rules of the Committee on Financial Services, we write to notify you of our intent to call additional witnesses selected by Committee Democrats to testify in continuation of the Full Committee hearing entitled, "Examining the Equifax Data Breach." Holding this hearing, also known as a "minority day hearing," in addition to the Majority's hearing on Thursday, October 5, 2017, will provide Members of the Committee and the American public the opportunity to consider and discuss ideas for ensuring the integrity of our country's consumer reporting system and safeguarding consumer data.

Given the scope of the cybersecurity breach, which has affected approximately 145.5 million consumers or nearly half the U.S. population, additional testimony from other credit reporting agencies and consumers, businesses, and financial institutions impacted by the breach are in order. Moreover, the hearing will also serve to present the public with policy solutions to the persistent problems plaguing our nation's credit reporting agencies.

Mr. Chairman, credit reporting agencies play an important role in the lives and financial futures of hardworking Americans. It is our duty, as Member of Congress, to fully examine how these agencies are operating and how they can be improved. That is why Democrats will exercise our right to hold a minority day hearing on the Equifax cybersecurity breach and we look forward to working with you to determine the date, time, and place of such hearing.

Sincerely,



Handwritten signatures of Maxine Waters, Joyce Beatty, and others, including a signature that appears to be "Hugo L. ...".

The Honorable Jeb Hensarling
 October 4, 2017
 Page 2 of 2

Hyde JS '76
 James Deane -

Jim Hayes
 Ed Jutkiewicz Cole #7

Stephen J. Ford
 Michael E. Capraro

Bill Foster

KK
 Al Moran

Robin Ant

AT
 [Signature]

J. H.
 Keith Bell

Bob Sherman

Charles B. Malone -

Wm Larry Clay

Danny Heck

Danett T. Killeo

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Ranking Member Maxine Waters

In your testimony you wrote that throughout your tenure as CEO of Equifax, your firm took data security and privacy extremely seriously, and that your company devoted substantial resources to it.

Waters Question #1: If this is the case, how is it possible that upon learning from the U.S. Department of Homeland Security's Computer Emergency Readiness Team of a key vulnerability in versions of software used by Equifax, your security team did not take any action in a timely manner? Doesn't the fact that no immediate action was taken upon being notified about a potential vulnerability by the Department of Homeland Security, suggest that your company didn't in fact take these issues that seriously?

A: As set forth below, the Equifax security team took immediate action upon being notified of a potential vulnerability. The breach occurred because of both human error and technology failures, not because Equifax failed to take these issues seriously.

On March 9, 2017, Equifax disseminated the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") notification internally by email requesting that personnel responsible for an Apache Struts installation immediately upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. Equifax now knows that the vulnerable version of Apache Struts existed within Equifax but was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 15, 2017, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. The scans, however, did not identify the Apache

Struts vulnerability. Unfortunately, Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability.

That said, Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Equifax's forensic consultants have recommended and are implementing a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also resigned from their positions.

Waters Question #2: In another example that underscores the low value your company placed on protecting consumers' data, researchers at a Wisconsin-based company called Hold Security discovered that an Equifax web portal was secured by the default username and password combination "admin and admin." Can you comment on how this type of easily-exploited password vulnerability was accepted at Equifax?

A: The use of such passwords was against Equifax policies. Further, Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies

on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Equifax's forensic consultants have recommended and are implementing a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Equifax has also implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017.

Waters Question #3: Your testimony notes that in addition to obtaining dispute documents from Equifax's online web portal, hackers "may have accessed a database table containing a large amount of consumers personally identifiable information (PII), and potential other data tables." Can you comment on why Equifax would ever find it necessary to store large amounts of consumers' sensitive personal information in a table that hackers could easily exploit?

A: Please see response to Waters Question #2.

Waters Question #4: I understand that on July 29th Equifax's security team identified "suspicious network traffic" as part of its online dispute portal. Is that correct? How do Equifax's internal documents or manuals providing guidance to its employees in this area define the term "suspicious" traffic? Does suspicious traffic suggest in any way that sensitive customer information may have been compromised?

A: On July 29, 2017, Equifax's security team observed suspicious network traffic associated with the U.S. consumer online dispute portal web application where consumers can upload documents or other information in support of a credit file dispute. In response, the security team investigated and immediately blocked the suspicious traffic that was identified. The security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. At that time, the security team did not recognize that any sensitive consumer PII had been compromised. The hard work to figure out the nature, scope, and impact of the hack then began, including whether personal identifying information ("PII") had been stolen. The term "suspicious traffic" is not defined in Equifax's relevant internal guidance documents.

Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental

report, and a final supplement. Equifax has provided these documents to the Committee previously.

Waters Questions #5.3 and #5.4: Does your internal legal department, or chief legal officer, have specified circumstances or even guidance in which that person is given authority to retain outside legal counsel relating to or because of a breach or unauthorized exposure of data? Does the cybersecurity team, or the chief information or security officer, have specific circumstances, or even guidance, in which that division or executive is authorized to retain an outside cybersecurity company?

A: As of May 2017, Equifax had in place several plans to address cybersecurity incidents and various types of crises. Among other topics, those plans contemplate retaining outside legal counsel and/or outside cybersecurity companies in connection with responding to a cybersecurity incident. For additional details regarding the plans and protocols in place to address a cybersecurity incident, please see the response to the question from Rep. Meeks provided below.

Waters Questions #7.1 and #7.2: Despite the sensitivity of the information that was compromised as part of the Equifax breach, which included names, Social Security Numbers, birth dates, addresses, and even driver's license numbers, and credit card information in some cases, Equifax did not opt to directly notify each of the affected individuals. Instead, Equifax has placed this burden on American consumers. Mr. Smith, do I have this right? Your current policy is that it is the victims' responsibility to determine whether they have been harmed, not the responsibility of the company that allowed their information to be stolen. Can you discuss how Equifax determined that it didn't need to notify affected consumers?

A: Equifax has notified consumers potentially impacted by this incident consistent with data breach notification laws. On September 7, 2017, Equifax provided notification of the incident by issuing a nationwide press release, providing a dedicated website where consumers could determine if they were impacted and sign up for a free credit file monitoring and identity theft protection product, and by providing a dedicated call center for consumers to obtain more information. The notification indicated that the incident impacted personal information relating to approximately 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.

Equifax also mailed written notices to consumers whose credit card numbers or dispute documents were impacted as well as to the approximately 2.5 million additional potentially impacted U.S. consumers identified since the September 7 announcement and notification.

In addition to Equifax's commitment to notify potentially affected consumers, Equifax provided notification pursuant to data breach notification statutes that impose various notice requirements for consumers. Equifax's notification included both substitute

notification contemplated by the data breach statutes using a nationwide press release, dedicated website, and call center, and through direct mail notification for certain groups of potentially impacted consumers.

Waters Question #8: In your written testimony, you wrote that “we at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data.” And you go on to say that you “apologize to the American people.” Mr. Smith, I’m sure the American people can appreciate that you are sorry, and I’m glad to hear that you understand that your firm is responsible for this compliance failure, but in addition to being “sorry” I’d like to know, who at your firm is actually being held accountable. To the extent that any executives who were directly responsible for addressing the vulnerability that had been identified by the Department of Homeland Security failed to do so, what specific changes has Equifax implemented to prevent this from occurring again?

A: At the time the breach was discovered, David Webb was Equifax’s Chief Information Officer, Susan Mauldin was Equifax’s Chief Security Officer, and Richard Smith was Equifax’s CEO. The individual who oversaw the team responsible for patching the relevant Apache Struts vulnerability on software supporting Equifax’s online disputes portal reported to Mr. Webb. Both Mr. Webb and Ms. Mauldin resigned from their positions, effective September 15, 2017 and Mr. Smith stepped down as CEO on September 25, 2017.

I would appreciate it if you could respond to my series of questions with a simple yes or no, given the short question and answer time period:

Waters Question #9.1: Is the current estimation from your company that 145.5 million American consumers have had their personally identifiable information and sensitive financial information, exposed to bad actors?

A: Yes, we currently estimate that 145.5 million consumers’ personal information was impacted. We believe 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, which Equifax will offer at the end of January.

Waters Question #9.2: Have your previous statements indicated that the company’s dispute complaint portal was the sole entry point in which consumers’ data was exposed?

A: Yes.

Waters Question #9.3: Does the fact that 145.5 million consumers’ data was exposed indicate that 145.5 million consumer complaints were submitted to Equifax?

A: No.

Waters Question #9.4: Let's end this confusion right now, did the firm's dispute complaint portal act as an open door that allowed bad actors to come into Equifax database in other areas that then resulted in the exposure of consumers' data outside of the dispute complaint portal because, otherwise, I'm confused about how the number of consumers has been determined?

A: Mandiant, a leading independent cybersecurity firm, provided Equifax with an executive summary, a supplemental report, and a final supplement, which collectively detail Mandiant's and Equifax's review process for determining the scope of data exposure for U.S. consumers. Equifax has provided these documents to the Committee previously.

Waters Question #18: On October 5, 2017, you testified that Equifax maintained a process for clearing the sale of Equifax securities by the company's officers. Please provide a detailed description of this process as it existed in August 2017. Did Equifax maintain a written policy reflecting this process? If so, please attach any and all documents in your possession evidencing a written policy. How did Equifax ensure that all relevant employees were aware of and adhered to this process? In your view, did these processes adequately prevent Equifax employees from trading Equifax securities in the days between insider awareness and public disclosure of a materially significant event?

A: The Board of Directors of Equifax released a report by the Special Committee of the Board of Directors on November 1, 2017, 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 is enclosed. In addition, a copy of the Insider Trading Policy is provided with this submission at Bates numbers EFXCONG-HFSC000000001–EFXCONG-HFSC000000014.

Equifax provides notification to all employees subject to pre-clearance requirements that a trading window is about to open and reminding these employees that they are subject to the company's insider trading policy and are required to pre-clear all transactions. The notification provided on July, 25, 2017 is provided with this submission at Bates numbers EFXCONG-HFSC0000000015–EFXCONG-HFSC0000000016. Equifax also provides a similar notification (absent reference to the pre-clearance requirement) to all employees that are permitted to trade only during the trading window.

Waters Question #24: Given that Equifax just lost the personally identifiable information for half of the U.S. adult population, I was surprised to learn that the Trump Administration just last week approved a contract for Equifax to "verify taxpayer identity" and "assist in ongoing identity verification and validations" on behalf of the IRS.

Given Equifax's clear inability to safeguard consumers' data, will you agree to reject this and enable the IRS to designate a different company for this contract?

A: On September 29, 2017, Equifax was awarded a bridge contract (task order number TIRNO-17-K-00497 issued against contract number GS00F159DA) to continue providing identification verification and validation services to the IRS while GAO was considering Equifax's protest of the IRS's award of a longer-term contract to provide those services. On October 12, 2017, Equifax received written notice from the IRS to stop work under the subject contract. On October 16, 2017, GAO denied Equifax's bid protest.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Keith Ellison

Ellison Question #9.1: It is my understanding that the short-term \$7.25 million contract awarded to Equifax was a bridge contract because of a contract dispute your former firm had with the IRS. The IRS wanted to bid the contract out to other vendors and Equifax disputed this change. So the bridge contract was to prevent a lapse in service during a protest on another contract. Is that information correct?

A: Please see response to Waters Question #24.

Ellison Question #9.2: On what basis did Equifax protest the IRS's action to rebid the contract?

A: Equifax's bid protest, which was filed on July 7, 2017, in accordance with 4 C.F.R. § 21.2(a)(2), enumerates Equifax's grounds for submitting the protest to GAO. Equifax protested because it believed IRS's evaluation was inconsistent with the terms of the solicitation. The basis of protest was two-fold. First, Equifax did not believe that Experian could meet the connection requirements described in the solicitation. Second, it appeared that Experian proposed to provide IRS with services that were materially different from the services required by the Solicitation. The protest alleged that IRS's evaluation, which found Experian technically acceptable notwithstanding these issues, was not conducted in accordance with the stated evaluation criteria. On October 16, 2017, GAO denied the bid protest.

Ellison Question #15: Was Equifax's market capitalization rate \$13.2 billion? If not, what was it?

A: In Equifax's most recent Form 10-Q securities filing, filed on November 9, 2017, the Company reported that it had approximately 120 million shares of common stock outstanding as of September 30, 2017. On October 2, 2017, which was the next day markets were open, Equifax's stock closed at \$107.81. Based on those values, Equifax had a market capitalization of approximately \$12.9 billion when the markets closed on October 2.

Ellison Question #16: Did Equifax earn \$3.1 billion of revenue last year? If not, how much in revenue did Equifax earn?

A: Equifax reported \$3.1 billion of operating revenue for twelve months ending on December 31, 2016 in its Form 10-K securities filing, filed on February 22, 2017.

Ellison Questions #17.1 and #17.2: Does Equifax have 9,500 employees? If not, how many employees does Equifax have?

A: As of December 1, 2017, Equifax has approximately 10,000 employees.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Denny Heck

Heck Question #1: When did Equifax first notify the Federal Bureau of Investigation about the breach?

A: Equifax notified the Federal Bureau of Investigation about the incident in question on August 2, 2017.

Heck Question #2: When did Equifax first notify a state law enforcement agency about the breach?

A: 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.

Heck Question #3: When did Equifax first notify the Federal Trade Commission about the breach?

A: Equifax notified the Federal Trade Commission about the incident in question on September 7, 2017.

Heck Question #4: When did Equifax first notify the Consumer Financial Protection Bureau about the breach?

A: Equifax notified the Consumer Financial Protection Bureau about the incident in question on September 7, 2017.

Heck Question #6: Will Equifax take any steps to reach out to all approximately 145 million people whose information was stolen in the hack? If not, how does it decide which people to attempt to directly notify and which to rely on media and people coming to the Equifax website?

A: Please see the response to Waters Questions #7.1 and #7.2.

Heck Question #10: Is Equifax taking any actions proactively to protect individuals whose information was stolen in the breach?

A: Equifax has taken a number of steps to notify and help protect individuals whose information was potentially impacted, including the following:

- Equifax created a website (www.equifaxsecurity2017.com) to notify and inform consumers about the incident. The website includes: (1) information about the incident; (2) a tool for consumers to learn if they were impacted; (3) identity theft

prevention tips; and (4) information about Equifax's free TrustedID Premier product.

- Equifax set up dedicated call centers to assist consumers affected by the incident. Since the incident was announced, Equifax has scaled up these operations to ensure it has more than enough associates to handle calls from concerned consumers.
- Until January 31, 2018, consumers can enroll in a free one-year product called TrustedID Premier, which includes:
 - Free credit monitoring with all three consumer credit bureaus;
 - Free access to Equifax credit reports for one year;
 - Free scanning of Social Security numbers against suspicious websites;
 - A free credit report lock feature; and
 - Identity theft insurance of up to \$1 million.
- By January 31, 2018, Equifax will offer a new service that will allow consumers to lock and unlock their Equifax credit file, for free, for life.

Heck Question #14: How has Equifax changed its process for patching vulnerabilities since discovering the breach?

A: Since discovering the breach, Equifax has improved its patching procedures to require a "closed loop" confirmation that necessary patches have been applied, rolled out a new scanner to identify vulnerabilities, upgraded its security technology, and increased accountability mechanisms for Equifax Security team members.

Heck Question #18: Equifax has stated that it identified records affected by reconstructing the queries used to access the database. What characteristics was the hacker searching for?

A: Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental report, and a final supplement. Equifax has provided copies of these documents to the Committee previously.

Heck Question #23: Does Equifax have written procedures laid out for notifying executives about a security breach?

A: As of May 2017, the company had in place several plans to address cybersecurity incidents and various types of crises, which include but are not limited to the following:

- A Security Incident Handling Policy & Procedures document, which dates back to 2008, and a Security and Safety Crisis Action Plan document, which dates back to 2013. These guides and plans were in place in May 2017 and have been updated and refined over time, including changes to the titles of the operative documents.
- A Crisis Management Plan (“CMP”), Parts I and II that has been in place dating back to 2013. The CMP plan covers a variety of crises, including data breaches.
- A Crisis Action Team (“CAT”) Plan specific to certain geographic regions within the Company. The CAT plan, like the CMP described above, covers a variety of crises, including data breaches.

Equifax faces numerous cyber threats every day. Its Cyber Threat Center (“CTC”) constantly assesses whether a particular threat can be resolved quickly by the Company’s own internal cybersecurity team, or whether the threat will require additional resources to remediate. If the CTC determines that a cybersecurity threat is unusual and will require additional resources to contain, it is typically designated a “Security Incident” and Equifax’s response outlined in the Security Incident Handling Policy & Procedures is triggered.

As set forth in the Security Incident Handling Policy & Procedures, once a Security Incident has been declared, its severity is classified based on a risk assessment including:

- number of affected systems;
- network impact;
- business services impact;
- sensitivity of information threatened or compromised; and
- the potential for harm.

Various senior officers, including those within the Legal Department, are notified by security of Security Incidents and typically outside experts are retained (e.g., a forensic team and outside counsel) to assist with the response.

Heck Questions #25 and #26: On what date was Chief Legal Officer John Kelley made aware of the breach? On what date did Chief Legal Officer approve the early August stock sales by other Equifax executives?

A: On July 30, 2017, Chief Legal Officer John Kelley was made aware of the fact that unusual activity had been detected on Equifax's network the prior evening, but neither he nor anyone else at the Company was made aware of the scope of the intrusion until mid-August when Mandiant and the Equifax security department began to determine the level of unauthorized activity. The Board of Directors of Equifax released a report by a Special Committee of the Board of Directors on November 1, 2017, 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, among other things, that that preclearance for the four trades was appropriately obtained and that each of the four trades at issue comported with Company policy.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Gregory Meeks

During the House Committee on Financial Services (“the Committee”) hearing on October 5, 2017, Mr. Rick Smith testified that: Equifax had written documentation on crisis management; Equifax would provide the Committee with crisis management documentation; and Equifax had tested it. By letter dated October 12, 2017, Representative Meeks requested from Equifax documentation of its written plan on how to respond to a breach and the dates when that plan was tested.

Following up on Mr. Smith’s testimony and in response to the letter from Representative Meeks, Equifax confirms that as of May 2017 the company had in place, and had tested, several plans to address cybersecurity incidents and various types of crises, which include but are not limited to the following:

- A Security Incident Handling Policy & Procedures document, which dates back to 2008, and a Security and Safety Crisis Action Plan document, which dates back to 2013. These guides and plans were in place in May 2017 and have been updated and refined over time, including changes to the titles of the operative documents. In June 2017, prior to Equifax’s detection of suspicious activity related to the cybersecurity incident, the company conducted a table-top test exercise of the “Security Incident Handling Policy & Procedures.” That test focused on the company’s Cyber Threat Center managing a newly announced Microsoft vulnerability.
- A Crisis Management Plan (CMP), Parts I and II that has been in place dating back to 2013. The CMP plan covers a variety of crises, including data breaches. A table-top test exercise of this plan was performed in June 2016, including a scenario that involved data security incident components.
- A Crisis Action Team (CAT) Plan specific to certain geographic regions within the Company. The CAT plan, like the CMP described above, covers a variety of crises, including data breaches. Table-top tests are also conducted for these plans, including scenarios involving data security incident components. The Southeast Crisis Action Team plan, for example, was activated in March 2017 in order to run an actual test of the plan.

Equifax is submitting examples of the crisis management documentation in place in May 2017 to the Committee (updates have been made to these plans since that time), Bates numbered EFXCONG-HFSC000000017–EFXCONG-HFSC000000187.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Kyrsten Sinema

Sinema Question #3: What changes has Equifax made to the IT department that failed to address the Apache Struts vulnerability? In addition to detailing any staff that were fired as a result, please provide a list of changes to company best practices to ensure that software patches are installed in the prescribed timeframe.

A: Please see response to Waters Questions #1, #2, and #8.

* * *

**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 of 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.

Appendix A**EQUIFAX'S SUBMISSION IN RESPONSE TO
COMMITTEE'S NOVEMBER 2, 2017 REQUESTS**

Please note that the question numbers provided in this Appendix track the question numbering in each Member's individual set of questions for the record. For the questions that Members provided without numbers, this Appendix assigns numbers to those questions for ease of reference.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Ranking Member Maxine Waters

Waters Question #4: I understand that on July 29th Equifax's security team identified "suspicious network traffic" as part of its online dispute portal. Is that correct? How do Equifax's internal documents or manuals providing guidance to its employees in this area define the term "suspicious" traffic? Does suspicious traffic suggest in any way that sensitive customer information may have been compromised?

Response: Equifax provided a response to Rep. Waters' question in its December 29, 2017 submission to the Committee. Equifax revises its answer to the Committee here:

On July 29, 2017, Equifax's security team observed suspicious network traffic associated with the U.S. consumer online dispute portal web application where consumers can upload documents or other information in support of a credit file dispute. In response, the security team investigated and immediately blocked the suspicious traffic that was identified. The security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. At that time, the security team did not have confirmation that sensitive consumer personal identifying information ("PII") had been compromised. The work to confirm the nature, scope, and impact of the hack then began, including confirming whether PII had been stolen. Over the next several weeks, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand these early indications of unauthorized activity on the network. By August 11, 2017, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the attackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables.

Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental report, and a final supplement. Equifax has provided these documents to the Committee previously.

Waters Questions ##5.1- 5.2: Despite identifying what you call “suspicious network traffic” on July 29th, Equifax waited until August 2nd to alert the FBI and hire an outside cyber security firm known as Mandiant to investigate the incident. How many other instances during your tenure as CEO with Equifax did the company hire an independent cybersecurity firm to investigate the scope, nature, and extent of the exposure of data caused by a breach or hack? How many times in your tenure did Equifax retain outside legal counsel to handle legal matters relating to a breach or unauthorized exposure of data?

Response: Equifax and its subsidiaries have never before experienced an intrusion involving U.S. consumer PII of the type and scale announced on September 7, 2017. In response to the Committee’s questions, Equifax focused on incidents investigated by Equifax’s Security team that involved the unauthorized access to or acquisition of U.S. consumer PII by one or more bad actors. Since January 1, 2015, Equifax has worked with independent cybersecurity firms to investigate two other such incidents, and retained outside legal counsel in connection with five other such incidents.

Waters Questions ##5.5 – 5.8: Did you decide to notify the FBI and hire an outside cyber firm because you believed that sensitive customer information may have been stolen? If so, when was this determination made? Was it made on July 29th, August 1st, or was that determination first made on August 2nd? Who, exactly, authorized or made the decision to notify the FBI and hire Mandiant?

Response: Equifax’s Vice President of Corporate Security and Safety notified the Federal Bureau of Investigation (“FBI”) about the cybersecurity incident on August 2, 2017, and managed communications with the FBI thereafter. Outside counsel has also been involved in communications with the FBI.

In August and September 2017, Equifax acted with diligence to secure and diagnose the suspicious activity observed on July 29 and 30. On August 2, consistent with its security incident response procedures, the Company: (1) retained the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; (2) engaged, through Company counsel, the independent cybersecurity forensic firm, Mandiant, to investigate the suspicious activity; and (3) contacted the FBI. It was not until well into August that Mandiant understood the scope of the consumer data impacted by the incident. Over the next several weeks, Mandiant and Equifax’s security department analyzed forensic data seeking to identify and understand these early indications of unauthorized activity on the network. Their task was to figure out what happened and what parts of the Equifax network were affected, identify consumers that were impacted, and determine what information was accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was not; it had stopped on July 30 when the portal was taken offline). Mandiant also helped

examine whether the data accessed contained PII, discover what data was exfiltrated from the Company, and trace that data back to unique consumer information.

Waters Questions ##6.1 – 6.2: As part of your written information security program as required by the FTC’s “Safeguards Rule,” do you also have a written breach notification policy outlining the circumstances when Equifax would notify customers affected by a breach? To the extent that you do have a written breach notification policy, does it state that Equifax would notify all affected customers whose sensitive personal information has may have been exposed, or does Equifax’s policy entail a specific harm threshold that must be met before notifying affected consumers?

Response: The Company had in place several plans to address cybersecurity incidents and various types of crises, which include but are not limited to the following:

- A Security Incident Handling Policy & Procedures document, which dates back to 2008, and a Security and Safety Crisis Action Plan document, which dates back to 2013. These guides and plans have been updated and refined over time, including changes to the titles of the operative documents.
- A Crisis Management Plan (“CMP”), Parts I and II, that has been in place dating back to 2013. The CMP plan covers a variety of crises, including information security incidents.
- A Crisis Action Team (“CAT”) Plan specific to certain geographic regions within the Company. The CAT plan, like the CMP described above, covers a variety of crises, including information security incidents.

Equifax faces numerous cyber threats every day. Its Cyber Threat Center (“CTC”) constantly assesses whether a particular threat can be resolved quickly by the Company’s own internal cybersecurity team, or whether the threat will require additional resources to remediate. If the CTC determines that a cybersecurity threat is unusual and will require additional resources to contain, it is typically designated a “Security Incident” and Equifax’s response outlined in the Security Incident Handling Policy & Procedures is triggered.

Waters Question #10: As you know, the Gramm-Leach-Bliley Act requires financial institutions, including consumer reporting agencies such as Equifax, to take steps to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of the information and to protect against access to or use of information which could result in substantial harm or inconvenience to any customer. In the wake of the massive breach at your company that exposed the sensitive personal information of half of the American population, I’d like to get a sense of who at Equifax you believe is ultimately responsible for compliance with the Gramm-Leach-Bliley Act?

Response: When Mr. Rick Smith appeared before the House Financial Services Committee on October 5, 2017, he testified: “As CEO at the time of the September 2017 security incident, I was ultimately responsible, and therefore, I have taken full responsibility.”

Waters Questions ##11.1-11.2: In your testimony you acknowledge that “human errors” and “technology failures” contributed to the breach that allowed criminals to access over 145 million Americans’ data. Who in your view is ultimately responsible for these human errors? Is it you?

Response: When Mr. Rick Smith appeared before the House Financial Services Committee on October 5, 2017, he testified: “As CEO at the time of the September 2017 security incident, I was ultimately responsible, and therefore, I have taken full responsibility.”

Waters Question #12.1: How many consumers have requested credit freezes after Sept 7, and how many before Sept 7?

Response: Between March 7, 2017 and September 7, 2017, approximately 52,482 U.S. consumers requested security freezes from Equifax. Between September 7, 2017 and May 4, 2018, approximately 3,203,476 U.S. consumers requested security freezes from Equifax.

Waters Question #12.2: Why did Equifax fail to promote credit freezes in response to earlier security breaches, but instead opt to sell credit monitoring services?

Response: Regardless of remediation products offered, credit freezes are available in accordance with state law. With regard to the 2017 cybersecurity incident, Equifax offered TrustedID Premier free for one year to all U.S. consumers, regardless of whether they were impacted by the incident. That set of consumer remediation tools included a year of free credit monitoring. Equifax also has waived any costs associated with placing, temporarily lifting, or permanently removing a security freeze on an Equifax credit file. On January 31, 2018, Equifax announced the availability of Lock & Alert, a new service that enables consumers to quickly lock and unlock their Equifax credit report using a computer or app downloaded on their mobile device. Lock & Alert is available for free, for life.

Waters Question #13: Is Equifax currently marketing and selling identity theft protection tools that contain similar functions as a “lock” that you have indicated the company plans to make available to every consumer, for free, starting in January 2018, and if so, how much is your company currently charging consumers for those services?

Response: Equifax is not currently marketing any paid consumer products.

Waters Question #14: Equifax's offer of credit monitoring services for a year, free credit freezes now, and a promise to provide a better product described as lock several months in the future, still fails to protect bad actors from using data exposed by your company to commit fraud because, to date, your company has not agreed to cover consumers' expenses to obtain credit freezes at the other two nationwide consumer reporting agencies--Experian and TransUnion. While it is true that there is no federal requirement for all the nationwide CRAs to provide vulnerable consumers and fraud victims the ability to obtain, temporarily lift, and permanently remove credit freezes, there should be a sense of corporate responsibility among the largest consumer reporting agencies in our country to do so immediately, given the massive breach that has occurred. To the extent that Experian and TransUnion have not stepped up to do so, I believe that it is mistake. But, to the extent, that all consumer credit bureaus have to have reasonable procedures in place to ensure, to the maximum extent possible, the accuracy of data on consumer reports, how is Equifax complying with this statutory obligation, after it has acknowledged that millions of American consumers' data has been exposed to bad actors?

Response: Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant did not find evidence of unauthorized access to Equifax's core consumer or commercial credit reporting databases, and the incident therefore did not impact the information Equifax provides for the calculation of consumers' credit scores.

Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges. Equifax now offers a new Lock & Alert service that allows consumers to lock and unlock their Equifax credit file, for free, for life. Equifax will also allow consumers to freeze and/or unfreeze their Equifax credit file for free, in compliance with the Economic Growth, Regulatory Relief, and Consumer Protection Act, S.2155, which was signed into law on May 24, 2018. Following the incident, Equifax also offered all U.S. consumers TrustedID Premier, a free package of services to substantially mitigate any risk of harm to consumers by helping to prevent unauthorized use of their personal information. Equifax will continue to work with the industry to improve the consumer experience with the national credit bureaus.

Waters Question #15: Has Equifax consulted with any consumer advocates or organizations since the public announcement of this breach to determine whether its method, mode, form, and delivery of information about the breach is being properly handled to mitigate consumers' confusion about what occurred and how to best protect themselves from harm caused by your firm's shoddy practices going forward?

Response: In response to the 2017 cybersecurity incident, Equifax devoted substantial resources to consumer notification and launched multi-faceted consumer resources, including the www.equifaxsecurity2017.com website and dedicated call centers, to provide consumers with information about the cybersecurity

incident and the various available products including TrustedID Premier, credit freezes, fraud alerts, and the Company's new Lock & Alert product. Since the announcement of the 2017 cybersecurity incident, Equifax has engaged in discussions with various stakeholders, including consumers, regulators, and other entities such as consumer advocacy groups. Equifax used the feedback regarding issues consumers were facing and questions consumers were asking to further inform its actions and took steps to address concerns raised by consumers and others. The Company enhanced the website to improve the customer experience by taking steps to make the website more user-friendly, updating the content on an ongoing basis, and adding new information to the Frequently Asked Questions section. The Company also added staff to its call centers and provided additional training to call center agents.

Waters Questions ##16.1 – 16.4: You have previously pointed to the Hurricanes as one of the reasons that Equifax call centers were not able to handle the capacity of consumers contacting the company after the breach. Yet, you have also pointed to the additional time the company needed to establish adequate mechanisms -- a separate website, for example -- as one of the reasons the firm waited until September 7th to announce publicly the massive breach. How many call center locations does Equifax currently have at its disposal? As part of the advance preparation the week of September 7th, did you visit any national news website, watch any national news media outlet, or otherwise read or become aware of what was a major news story on almost all television, internet, and other outlets, about the risk of Hurricanes that were likely going to make landfall in the United States? Yes or no, were you and other senior executives at Equifax, unaware of the Hurricanes that were being forecasted to hit this country in the days before September 7th? Why did Equifax not anticipate that the call centers located in certain areas, could be adversely impacted by natural disasters and make alternative arrangements?

Response: The extent to which individual Equifax employees were aware of weather forecasts relating to hurricane activity varied. During the period prior to the September 7, 2017 announcement of the breach, Equifax was focused on the forensic investigation, the identification of potentially impacted consumers, and the development of a comprehensive consumer support package.

Equifax utilized five call centers to handle the call volume relating to the 2017 cybersecurity incident. These included two existing call centers and three additional call centers. Equifax also increased internal trunk capacity at the call centers.

Prior to the September 7, 2017 announcement of the breach, Equifax added approximately 770 incremental call center agents. On September 7, 2017, Equifax added additional call center agents, bringing the total number of incremental call center agents to approximately 1,350. To handle the unprecedented call volume following the announcement of the breach, Equifax continued to increase call center staffing. By October 6, 2017, Equifax had added another 2,045 agents to

handle authentication and servicing issues, bringing the total number of incremental call center agents to approximately 3,400. Equifax also continuously solicited overtime and double shifts to increase utilization of call center agents.

Waters Question #17: During questioning at the House Energy and Commerce Committee hearing held earlier this week, you admitted that although Equifax is providing free credit monitoring to affected consumers, you are simultaneously selling such service to companies such as “Life Lock” that contract with your company to provide identity theft monitoring services. If you’re willing to provide this service to consumers for free, why are you steering vulnerable and worried consumers to purchase the same type of service through a third-party vendor, one in which Equifax receives financial benefits from?

Response: In April 2016, Equifax partnered with LifeLock to provide data for LifeLock’s identity protection services. Equifax has not increased its profits from its partnership as a result of the cybersecurity incident announced on September 7, 2017. Any marginal increase in revenue from Equifax’s relationship with LifeLock is more than offset by the drop in revenue that comes from offering a consumer support package to all U.S. consumers with credit files, regardless of whether they were impacted by the cybersecurity incident. This included a complimentary, one-year subscription to a credit file monitoring and identity theft protection product. Equifax established a website where U.S. consumers were able to receive further information about the breach, determine if they were potentially impacted by the breach, and enroll in TrustedID Premier (www.equifaxsecurity2017.com). Equifax also established a dedicated call center to assist consumers with questions. The enrollment period for TrustedID Premier was extended until January 31, 2018, when Equifax launched its new Lock & Alert service, which allows consumers to control access to their Equifax credit file directly—for free, for life. Equifax also waived the fee to add, lift, or permanently remove a security freeze on an Equifax credit file. The waiver of fees associated with security freezes of Equifax credit files has been extended indefinitely, in compliance with the Economic Growth, Regulatory Relief, and Consumer Protection Act, S.2155, which was signed into law on May 24, 2018.

Waters Questions ##19.1-19.2: In your October 5, 2017 written testimony, you testified that Equifax first observed suspicious network activity on July 29, 2017. This activity was observed again on July 30, 2017, leading to Equifax’s security department shutting down the company’s consumer dispute website. However, Equifax did not notify the public of any changes to its cybersecurity risks until six weeks later on September 7 when it disclosed a major breach of consumer data. Please describe your understanding of Equifax’s obligations to notify the public of significant changes in the company’s cybersecurity risks. During your time as CEO, what factors did Equifax’s management consider in determining whether and when to publicly report any cybersecurity incidents?

Response: The Company considers a variety of factors in determining whether and when to provide notice of or otherwise disclose a cybersecurity incident, including the

materiality of the incident, whether the Company has legal and/or contractual obligations to notify, whether sensitive consumer information was accessed as a result of the security incident, whether PCI data was accessed as a result of the security incident, whether there are any consumers to whom substantial harm or inconvenience could result due to the unauthorized access or use of their sensitive consumer information, and whether the Company has been requested by law enforcement to delay notification.

Waters Question #19.3: You testified on October 5, 2017 that Equifax maintained a protocol that set forth the Equifax's procedures for notifying regulators, attorneys general, and consumers of cybersecurity incidents. Please provide a detailed description of each step in the protocol governing Equifax's response to the breach announced on September 7, 2017. Attach any and all relevant documents in your possession evidencing the protocol referenced in your October 5, 2017 testimony.

Response: Equifax provides notifications, as appropriate, based on applicable laws and the unique facts of a given security incident. Equifax's Security Incident Handling Policy & Procedures document addresses the general procedures for notifying consumers and law enforcement. That document was produced to the Committee on January 2, 2018, at Bates numbers EFXCONG-HFSC000000139–EFXCONG-HFSC000000187. Additional plans for addressing cybersecurity incidents and various types of crises were also provided to the Committee on January 2, 2018, at Bates numbers EFXCONG-HFSC000000017–EFXCONG-HFSC000000187.

Waters Question #20: What specific actions have you taken to help consumers who have been impacted by Hurricanes Maria, Harvey, or Irma?

Response: Equifax did not take specific actions in regard to creating special remediation tools for consumers potentially impacted by the hurricanes, although the company regularly works with financial institutions and other data furnishers to appropriately describe external factors in a consumer's credit report that may contribute to a consumer's payment behavior. On September 7, 2017, Equifax rolled out a consumer support package to all U.S. consumers, regardless of whether they were impacted by the breach or their location. This included a complimentary, one-year subscription to a credit file monitoring and identity theft protection product. Equifax established a website where U.S. consumers were able to receive further information about the breach, determine if they were potentially impacted by the breach, and enroll in TrustedID Premier (www.equifaxsecurity2017.com). Equifax also established a dedicated call center to assist consumers with questions. The website and call center provide Spanish language options. The enrollment period for TrustedID Premier was extended until January 31, 2018, when Equifax launched its new Lock & Alert service, which allows consumers to control access to their Equifax credit file directly—for free, for life. Equifax also waived the fee to add, lift, or permanently remove a security freeze on an Equifax credit file. The waiver of fees associated with

security freezes of Equifax credit files has been extended indefinitely, in compliance with the Economic Growth, Regulatory Relief, and Consumer Protection Act, S.2155, which was signed into law on May 24, 2018.

Waters Questions #21-22: Has Equifax complied with any state laws or regulations that require the company to notify specific individuals who have had their data exposed in this breach? What specific measures is Equifax taking to ensure that residents in areas affected by the Hurricanes are: (1) aware of the massive breach that has occurred; (2) have information about how to access the remedies that Equifax is making available for free in response; (3) and to the extent that one of those areas has a large Spanish-speaking community, what additional, specific actions has the firm done to make sure that disclosures are available in languages spoken in the United States beside English, like Spanish; (4) in an area, like PR that has been devastated by a hurricane, how is Equifax ensuring those residents are aware of the breach and can take remedial actions, when many of the residents are struggling with meeting their basic survival needs now and don't have access to the internet or even telephones?

Response: Equifax issued a nation-wide press release on September 7, 2017 to provide substitute notice to U.S. consumers in accordance with state data breach notification laws. As of that date, U.S. consumers could access the website established by Equifax, www.equifaxsecurity2017.com, to receive further information about the breach, inquire as to whether they may have been impacted, and enroll in TrustedID Premier. Equifax also established a dedicated call center to assist consumers with questions. The website and call center provide Spanish language options. The call center is able to assist consumers who do not have internet access.

On September 7, 2017, Equifax also provided written notification to the Attorneys General of all 50 states, the District of Columbia, and Puerto Rico.

Equifax has also mailed written notification to certain groups of impacted consumers. On October 2, 2017 Equifax announced that the cybersecurity firm Mandiant completed the forensic portion of its investigation of the cybersecurity incident disclosed on September 7 to finalize the consumers potentially impacted. The completed review determined that approximately 2.5 million additional U.S. consumers were potentially impacted. Updated notification was provided to all state Attorneys General regarding these additional potentially impacted consumers on October 12, 2017. To minimize confusion, Equifax mailed written notices, beginning on October 13, to all of the additional potentially impacted U.S. consumers identified after the September 7 announcement. Equifax also sent individual direct mail notices beginning on October 23, 2017 to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. On March 1, 2018, Equifax announced that the Company had confirmed the identities of U.S. consumers whose partial driver's license information was taken. Through additional efforts, Equifax was able to identify

approximately 2.4 million U.S. consumers whose names and partial driver's license information were stolen, but who were not in the previously identified affected population discussed in the Company's prior disclosures about the incident. Equifax is in the process of mailing notification letters to these newly identified consumers directly, and will offer identity theft protection and credit file monitoring services at no cost to them. Information about registering for these services will be included in the notification.

Waters Question #23: Will Equifax implement a program where any consumer in designated natural disaster zones for Hurricanes Maria, Harvey or Irma can request to have any negative reporting removed or scrubbed from their file at Equifax from the date of the disaster for a 1-year period?

Response: Consumers in areas impacted by Hurricanes Maria, Harvey, and Irma have access to the comprehensive consumer support package Equifax offered to all U.S. consumers, regardless of whether they were impacted by the breach or their location. This included a complimentary, one-year subscription to TrustedID Premier, a credit file monitoring and identity theft protection product. The enrollment period for TrustedID Premier was extended until January 31, 2018, when Equifax launched its new Lock & Alert service, which allows consumers to control access to their Equifax credit file directly—for free, for life.

Equifax also waived the fee to add, lift, or permanently remove a security freeze on an Equifax credit file. The waiver of fees associated with security freezes of Equifax credit files has been extended indefinitely, in compliance with the Economic Growth, Regulatory Relief, and Consumer Protection Act, S.2155, which was signed into law on May 24, 2018.

Equifax also has a dispute mechanism for consumers to dispute information on their credit files that they believe to be inaccurate. Consumers in areas impacted by Hurricanes Maria, Harvey, and Irma can dispute information in their credit files by phone, by mail, or online.

Waters Question #25: Please provide a state-by-state breakdown, as well as a breakdown by Congressional District of the U.S. House of Representatives, of consumers who potentially had their personal information exposed in the data breach.

Response: Equifax publicly disclosed on September 7 and October 2, 2017 that the attackers accessed certain information related to approximately 145.5 million consumers. The chart below indicates the approximate number of affected residents in this population by state. Equifax does not have a breakdown of affected by consumers by congressional district.

| State | Approx. # of Affected Residents Identified in Sept. & Oct. 2017 |
|-------|---|
| AK | 262,120 |
| AL | 2,305,073 |
| AR | 1,307,321 |
| AZ | 2,890,367 |
| CA | 15,606,038 |
| CO | 2,528,768 |
| CT | 1,546,289 |
| DC | 356,566 |
| DE | 444,671 |
| FL | 11,028,946 |
| GA | 5,320,307 |
| HI | 462,195 |
| IA | 1,125,396 |
| ID | 671,408 |
| IL | 5,514,543 |
| IN | 3,904,161 |
| KS | 1,129,387 |
| KY | 1,895,825 |
| LA | 2,166,568 |
| MA | 2,982,421 |
| MD | 3,007,916 |
| ME | 536,436 |
| MI | 4,463,878 |
| MN | 2,101,374 |
| MO | 2,621,279 |
| MS | 1,315,829 |
| MT | 377,052 |
| NC | 4,520,059 |
| ND | 253,511 |
| NE | 742,937 |
| NH | 634,614 |
| NJ | 4,038,679 |
| NM | 863,486 |
| NV | 1,305,079 |
| NY | 8,447,480 |
| OH | 5,269,059 |

| State | Approx. # of Affected Residents Identified in Sept. & Oct. 2017 |
|-------|---|
| OK | 1,729,826 |
| OR | 1,762,762 |
| PA | 5,548,576 |
| PR | 1,023,564 |
| RI | 495,177 |
| SC | 2,419,033 |
| SD | 285,239 |
| TN | 3,114,423 |
| TX | 12,210,497 |
| UT | 1,230,170 |
| VA | 4,110,631 |
| VT | 247,607 |
| WA | 3,243,664 |
| WI | 2,201,666 |
| WV | 741,624 |
| WY | 240,189 |

As Equifax stated in its March 1, 2018 press release, Equifax was also able to identify approximately 2.4 million U.S. consumers whose names and partial driver's license information were stolen, but who were not in the previously identified population discussed in the Company's prior disclosures about the incident. At this time, the Company has been able to identify approximate state-by-state counts based on available address information for approximately 1.7 million of these consumers. The chart below indicates the approximate number of affected residents in this population by state based on currently available information. Equifax does not have a breakdown of impacted consumers by congressional district.

| State | Approx. # of Affected Residents Identified in March 2018 |
|-------|--|
| AK | 5,634 |
| AL | 19,359 |
| AR | 15,970 |
| AZ | 30,427 |
| CA | 208,971 |
| CO | 24,407 |

| State | Approx. # of Affected Residents Identified in March 2018 |
|-------|--|
| CT | 28,902 |
| DC | 4,183 |
| DE | 4,044 |
| FL | 105,628 |
| GA | 47,697 |
| HI | 7,464 |
| IA | 5,920 |
| ID | 6,113 |
| IL | 50,460 |
| IN | 27,747 |
| KS | 9,271 |
| KY | 12,909 |
| LA | 30,644 |
| MA | 33,398 |
| MD | 29,276 |
| ME | 5,832 |
| MI | 211,975 |
| MN | 19,621 |
| MO | 23,507 |
| MS | 17,563 |
| MT | 3,389 |
| NC | 35,442 |
| ND | 2,890 |
| NE | 4,514 |
| NH | 5,077 |
| NJ | 43,943 |
| NM | 8,730 |
| NV | 17,189 |
| NY | 95,088 |
| OH | 41,390 |
| OK | 17,687 |
| OR | 25,421 |
| PA | 49,202 |
| PR | 61,865 |
| RI | 5,646 |
| SC | 19,038 |

| State | Approx. # of Affected Residents Identified in March 2018 |
|-------|--|
| SD | 3,159 |
| TN | 26,120 |
| TX | 161,311 |
| UT | 20,185 |
| VA | 31,612 |
| VT | 3,812 |
| WA | 27,105 |
| WI | 20,421 |
| WV | 6,441 |
| WY | 3,315 |

Waters Question #26: How many consumers to date have you proactively and individually sent notifications to that their personal information was exposed through the data breach?

Response: Please see response to Question #21.

Waters Question #27: Why does it take 48 hours to obtain a credit lock or freeze provided as a remedy for consumers whose personal information was exposed? What is the average amount of time it takes for the company to process these requests?

Response: The scale of this incident was enormous, and Equifax struggled with the initial volume of consumers utilizing its call centers and website. Equifax is continuously working to enhance and improve consumers' experience with the incident website, www.equifaxsecurity2017.com. The Company created more intuitive navigation on the microsite and reduced the number of phone numbers listed. Following the initial launch of the "Am I impacted?" search tool on September 7, 2017, the Company resolved some technical issues with the search functionality. Following the completion of a forensic investigation on October 2, 2017, the Company is now able to provide a more definite impact response to U.S. consumers that take advantage of the "Am I impacted?" search tool, which can be accessed by going to the home page of the site.

In addition, following completion of the forensic investigation on October 2, 2017, the Company has:

- Mailed written notices to the approximately 2.5 million additional U.S. consumers that were potentially impacted; and
- Updated the "Am I impacted?" search tool on the website to include the entire impacted population of approximately 145.5 million U.S. consumers.

Waters Questions ##28.1 – 28.3: What company, if any, does Equifax have cybersecurity or data breach insurance? What are the terms and conditions of any such contract? What company, if any, does Equifax have cybersecurity or data breach insurance?

Response: Equifax has maintained dedicated cyber coverage since at least August 1997. The amounts, policy retentions, and terms and conditions of Equifax's cyber insurance have changed at annual policy renewals over the last several years.

Waters Question #28.4: Was a risk predictor or score used by this company in the underwriting and rating of this contract and, if so, what was the name of the credit scoring developer that generated the model used to produce this risk predictor or score, what was the range of available risk predictors or scores, and what was the risk predictor or score associated with your company, the reasons provided that may have adversely impacted this risk predictor or score, the date in which this risk predictor or score was generated, and the number of the risk predictor or score?

Response: The Company is unaware of any scoring that its insurers may have used in the underwriting of the cyber policies.

Waters Question #29: Please provide a copy of the calendar of scheduled events for the current interim CEO for October 4-October 6, 2017, and from October 24, 2017 – October 26, 2017.

Response: The Company will coordinate with Committee staff regarding this document request.

Waters Question #30: Please provide the exact dates, times, method of delivery, full name, job title or position, name of the office or division, in which the company notified any state law enforcement agency about this breach along with a copy of the exact text, if in written form, or outline, script, or other notes, if provided through the telephone.

Response: As discussed above in response to Question #5.5, Equifax notified the Federal Bureau of Investigation about the incident in question on August 2, 2017.

On September 7, 2017, Equifax mailed notification letters to attorneys general for 52 states and U.S. territories. The notification letter stated:

I write on behalf of Equifax Inc. ("Equifax") regarding a cybersecurity incident potentially impacting information relating to approximately 143 million U.S. consumers. The approximate number of potentially impacted residents in your state is identified in Exhibit B. Equifax takes seriously its responsibility to protect the security of personal information, and our priority is to assist consumers who may have been impacted. The circumstances of the incident and the steps Equifax is taking to protect consumers are set forth below.

On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files. Upon discovery, Equifax acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. The company has found no evidence of unauthorized access on Equifax's core consumer or commercial credit reporting databases.

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to notify consumers of the incident, help them understand if they were potentially impacted, and provide steps they can take to protect against the potential misuse of their information. In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted.

Equifax is also offering to all U.S. consumers complimentary credit file monitoring and identity theft protection for one year, even if a consumer is not impacted by this incident. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers. Information on how to enroll for this offering is included on the dedicated website. Additionally, Equifax has established a dedicated call center, 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week, to answer questions about the incident, assist consumers in signing up for the complimentary service, and provide information about how to further protect personal information.

Please do not hesitate to contact me if you have any questions regarding this notification.

For certain states, Equifax also submitted required digital notification forms.

Waters Question #31: Please provide the exact dates, times, method of delivery, full name, job title or position, name of the office or division, in which the company notified TransUnion, Experian, VantageScore, or any of these company's affiliates or subsidiaries about this breach, along with a copy of the exact text, if in written form, or outline, script, or other notes, if provided through the telephone.

Response: TransUnion, Experian, and VantageScore learned about the breach contemporaneously with the public, by the press release published on September 7, 2017.

Waters Question #32: How many full-time employees are responsible for cybersecurity or data security at Equifax or its subsidiaries or affiliates, as of January 1, 2017, at 9 a.m. (EST)?

Response: On January 1, 2017, the Equifax Security department had approximately 187 full-time employees, although other employees are also regularly engaged in information security, including members of the Equifax Technology, Data and Analytics, and Compliance teams. Equifax also uses third parties to assist with information security efforts.

Waters Question #33: Who is the most senior person at Equifax, its affiliates or subsidiaries, responsible for ensuring the safeguarding of consumers' nonpublic personal information collected and maintained at the company, what was this annual salary for the person in this position in 2015, 2016, and this year, and what other forms of monetary or non-monetary compensation provided to this person in 2015, 2016, and this year? Please provide the description of the responsibilities and other duties of this position.

Response: Rick Smith as Chairman and CEO was the most senior person at Equifax responsible for ensuring the safeguarding of consumers' nonpublic personal information. For a detailed description of Mr. Smith's 2016 compensation, as well as relevant considerations related to his compensation, please see Equifax's 2017 Proxy Statement. For information regarding Mr. Smith's 2015 compensation and relevant considerations, please see Equifax's 2016 Proxy Statement. Both proxy statements are available in the Investor Relations section of the Equifax website, as well as through the U.S. Securities and Exchange Commission's EDGAR database of securities filings.

Waters Question #34: Please list and provide the narrative and description, as it appears on the website of Equifax, and the exact dollar amount, including any applicable state or federal sales tax, for any consumer product or services that was marketed to and made available for purchase, to consumers relating to any credit monitoring or identity theft protection service or product, as of 6 p.m. (EST) on September 7, 2017, from the current date, including any credit or security freezes, the cost to obtain a credit record for the sole purpose of obtaining a credit or security freeze for any minor. Please specify the amount of revenue, with a specific breakdown by each credit monitoring product or service that

Equifax, its affiliates or subsidiaries, have earned as of 6 p.m. (EST) as of September 7, 2017, to the current date.

Response: Following the announcement of the 2017 cybersecurity incident, Equifax removed all subscription consumer products from its website and is not currently marketing any paid consumer products. The Company offered the TrustedID Premier product free to all U.S. consumers for a year regardless of whether they were impacted by the 2017 cybersecurity incident. TrustedID Premier is a free service that includes copies of a consumer's Equifax credit report. For consumers who are not enrolled in TrustedID Premier, the cost for obtaining a copy of their credit report is in accordance with state law. Equifax also has waived any costs associated with placing, temporarily lifting, or permanently removing a security freeze on an Equifax credit file.

Waters Question #35: Did Equifax, its subsidiaries or affiliates, contacted or discussed with any employee in its internal legal or counsel department or outside counsel or legal advisor, how to, or the possibility, or whether to consider, filing for bankruptcy under any relevant state law?

Response: The impact of the 2017 cybersecurity incident on the Company's financial condition was set forth in the Form 10-K filed with the Securities and Exchange Commission on March 1, 2018:

Through December 31, 2017, the Company recorded \$113.3 million of pretax expenses related to the cybersecurity incident. We have included \$14.2 million of these expenses in cost of services and \$99.1 million in selling, general and administrative expenses in the accompanying Consolidated Statements of Income for the year ended December 31, 2017. Expenses include costs to investigate and remediate the cybersecurity incident and legal and other professional services related thereto, all of which were expensed as incurred.

We expect to incur significant legal and other professional services expenses associated with the cybersecurity incident in future periods. We will recognize these expenses as services are received. Costs related to the cybersecurity incident that will be incurred in future periods will also include increased expenses and capital investments for IT and security. We expect to incur increased expenses for insurance, finance, compliance activities, and to meet increased legal and regulatory requirements. We will also incur increased costs to provide free services to consumers including increased customer support costs.

The 10-K also sets forth certain risk factors related to the 2017 cybersecurity incident, including:

- 1) *Security breaches like the cybersecurity incident announced in September 2017 and other disruptions to our information technology infrastructure could compromise Company, consumer and customer information, interfere with our operations, cause us to incur significant costs for remediation and enhancement of our IT systems and expose us to legal liability, all of which could have a substantial negative impact on our business and reputation.*

Because our products and services involve the storage and transmission of personal information of consumers, we will continue to routinely be the target of attempted cyber and other security threats by outside third parties, including technically sophisticated and well-resourced bad actors attempting to access or steal the data we store. Insider or employee cyber and security threats are also a significant concern for all companies, including ours. In addition, the 2017 cybersecurity incident may embolden individuals or groups to target our systems. We must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. If we experience additional breaches of our security measures, including from incidents that we fail to detect for a period of time, sensitive data may be accessed, stolen, disclosed or lost. Any such access, disclosure or other loss of information could subject us to significant additional litigation, regulatory fines, penalties, losses of customers or reputational damage, any of which could have a significant negative impact on our cash flows, competitive position, financial condition or results of operations. We expect our insurance coverage will not be adequate to compensate us for all losses that may occur due to the 2017 cybersecurity incident and we cannot ensure that our insurance policies in the future will be adequate to cover losses from any future failures. In addition, our third-party insurance coverage will vary from time to time in both type and amount depending on availability, cost and our decisions with respect to risk retention.

- 2) *The government investigations and litigation resulting from the 2017 cybersecurity incident will continue to adversely impact our business and results of operations.*

The claims and investigations have resulted in the incurrence of significant external and internal legal costs and expenses and reputational damage to our business and are expected to continue throughout 2018 and beyond. The resolution of these matters may result in damages, costs, fines or penalties substantially in excess of our insurance coverage, which, depending on the amount, could have a material adverse effect on our liquidity or compliance with our credit agreements. If such damages, costs, fines or penalties were great enough that we could not pay them through funds generated from operating activities and/or cause a default under our revolving credit facility, we may be forced to renegotiate or obtain a waiver under our revolving credit facility and/or seek additional debt or equity financing. Such renegotiation or financing may not be available on acceptable terms, or at all. In these circumstances, if we were unable to obtain sufficient financing, we may not be able to meet our obligations as they come due. The outcome of such claims and investigations could also adversely affect or cause us to change how we operate our business. The governmental agencies investigating the cybersecurity incident may seek to impose injunctive relief, consent decrees, or other civil or criminal penalties, which could, among other things, impact our ability to collect and use consumer information, materially increase our data security costs and/or otherwise require us to alter how we operate our business. Any legislative or regulatory changes adopted in reaction to the cybersecurity incident or other companies' data breaches could require us to make modifications to the operation of our business that could have an adverse effect and/or increase or accelerate our compliance costs. Furthermore, these matters necessitate significant attention by management, which may divert the focus of management from the operation of our business resulting in an adverse impact on our results of operations.

- 3) *The cybersecurity incident and the adverse publicity that followed have had a negative impact on our reputation, and we cannot assure it will not have a long-term effect on our relationships with our customers, our revenue and our business.*

See Equifax 10-K filing, March 1, 2018, pp. 14-16.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Keith Ellison

The last time this Committee met to discuss issues important to Equifax, we were asked to consider a bill H.R. 2359, the "Fair Credit Reporting Act Liability Harmonization Act." We met on Thursday, September 7th at 10 a.m. H.R. 2359 was introduced by Congressman Loudermilk (R-GA) with support from 12 Republicans on the Financial Services Committee.

The morning of September 7th, Equifax supported this bill because if the law was changed, Equifax could avoid paying punitive damages. As I understand it, this bill would make sure that Equifax paid no more than \$500,000 in a class action lawsuit because of willful or reckless act that violated the law or caused injuries to a consumer which could include a massive data breach.

So on the morning of Thursday, September 7th Equifax and the Republican leadership brought forward a bill to help Equifax avoid paying punitive damages in case it harmed consumers as a class. But by 5 pm on that same day, Thursday, September 7th, Equifax announced a breach exposing the personal information of 145 million people. Obviously, the cap of \$500,000 in damages ensures that the 145 million people affected by this breach would get absolutely nothing. Not one penny in damages.

Ellison Question #1.1: Does Equifax still support Mr. Loudermilk's bill, H.R. 2359?

Response: Equifax continues to support legislation that promotes consistency among the federal consumer protection laws.

Ellison Question #1.2: If Mr. Loudermilk's bill became law, how would that affect Equifax's liability in case of a massive data breach or other types of injuries to people whose credit information Equifax collects?

Response: Data breach litigation is typically brought under state negligence and breach notification laws. All fifty states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have such laws. Litigation is also often pursued under contract law, unfair or deceptive acts or practices laws, or other violations of statutory or common law. Under such laws, Equifax's liability would not be capped.

The FCRA Liability Harmonization Act amends the Fair Credit Reporting Act (FCRA), the law that ensures the credit reporting system is fair and accurate. The purpose of the FCRA is "to require that 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." 15 U.S.C. § 1681(b).

The FCRA Liability Harmonization Act would establish a reasonable limit on liability in FCRA class action lawsuits consistent with caps that exist in other financial consumer protection laws. If the bill were to become law, consumers could continue to exercise their rights under the FCRA with the possibility of being awarded actual damages, statutory damages, attorney's fees, and the costs of the action. Because breach cases typically do not implicate or rely on allegations related to the FCRA, the bill would not generally impact a consumer's ability to recover damages.

When the breach occurred, there was an outcry that Equifax's credit monitoring service required people to consent to mandatory pre-dispute arbitration. Consumers should not be forced to "go it alone" in a system tilted to benefit Equifax. I was glad to hear that the forced arbitration clause was removed although I am hearing experts say that some of the fine print in the credit freeze, monitoring and lock services contain arbitration clauses.

Ellison Question #2: Can you confirm that people signing up for credit monitoring and lifetime credit lock through Equifax are not going to be subject to "forced arbitration clauses?"

Response: On September 11, 2017, Equifax issued a notice confirming that enrolling in TrustedID Premier, the free credit file monitoring and identity theft protection product Equifax offered to all U.S. consumers, did not waive any rights to take legal action. The Terms of Use for the new Lock & Alert product do not contain an arbitration clause and clearly state that no arbitration clause will ever be added to the Terms of Use for this product.

Ellison Question #3: Can you confirm that "forced arbitration clauses" are not being used in your general terms of service?

Response: Equifax is not currently offering any subscription services to consumers for purchase. Equifax does not include an arbitration clause in connection with the Lock & Alert application that became available in January 2018.

Ellison Question #4: When you testified before the Senate, you told Senator Chris Van Hollen that you were unaware of any lobbying for a bill that would repeal the Consumer Financial Protection Bureau's rule protecting consumers from class action bans and forced arbitration clauses. Yet, in reviewing your Lobbying Disclosure Forms, inserted below, Equifax spent nearly \$3 million in lobbying expenses that included lobbying on "use of arbitration clauses" in "consumer financial products and services." Did Equifax expend resources to repeal the CFPB's rule protecting consumers from class action bans? Did the governmental affairs staff of Equifax educate and/or advocate against the CFPB's arbitration rule?

Response: The government affairs staff had limited engagement and spent de minimis expenses in advocacy regarding the arbitration rule. Lobbyists employed by Equifax attended two industry-wide meetings on July 11, 2017 with the Senate regarding several topics impacting the credit reporting industry, including the use of arbitration agreements and House Joint Resolution 111. Equifax also participated in industry-wide calls in which the topic of arbitration clauses was addressed.

Expenditures for these meetings were limited to travel costs and salary for lobbyists employed by Equifax. External consultants and lobbyists are generally on monthly retainer arrangements and only reimbursed incidental, negligible costs for individual meetings.

After this breach, two senior executives—the Chief Information Officer and the Chief Security Officer—decided to quote, “retire, effective immediately.” This raises all sorts of questions about the executives’ role in the data breach, and whether or not they retired so they could obtain or retain compensation that otherwise may have been forfeited.

Ellison Question #5: Do you think it makes sense that these officials were allowed to retire? Should they have any of their incentive compensation clawed-back?

Response: Having the former Chief Information Officer and Chief Security Officer available to the Company was important to prevent loss of institutional knowledge as Equifax restructured its data security functions.

The Company’s compensation clawback policy is outlined in the public proxy statement available on Equifax’s website. The policy is triggered in the event of a material restatement of the Company’s financial results. The cybersecurity incident disclosed on September 7, 2017, did not result in the restatement of financial results. The Board of Directors has created a Special Committee that is examining compensation questions. Furthermore, the Board of Directors adopted a revised claw-back policy for the 2018 executive compensation program that would allow the Board to recover incentive compensation in the event of misconduct or failure of oversight that results in significant financial or reputational harm.

Ellison Question #6: As I understand it, Equifax’s executive compensation system excludes the cost of legal settlements from the way it calculates incentive pay. So executives are not penalized for mismanagement that leads to expensive litigation. Is that true? Why would Equifax structure its compensation system that way?

Response: As discussed in Equifax’s 2018 Proxy Statement, with respect to 2017 compensation, the Board of Directors determined that members of Equifax’s senior leadership team would not receive any annual cash incentive compensation for 2017 even though performance measures were achieved. Further, with respect

to the other participants in the 2017 annual cash incentive plan, the Board's Compensation Committee adjusted corporate adjusted earnings per share to add back expenses related to the 2017 cybersecurity incident for incentive measurement purposes.

Going forward, the Board made several important changes to the 2018 executive compensation program in response to the 2017 cybersecurity incident. Specifically, the Board revised the Company's compensation clawback policy to add a financial and reputational harm standard. Under the revised policy, the Board may recover incentive compensation awarded to employees in the event of misconduct or failure of oversight that results in significant financial or reputational harm. Additionally, the Board added a cybersecurity performance measure as one of the metrics to evaluate performance of all employees, including executives, under the 2018 annual bonus plan. Achievement of this cybersecurity metric cannot increase an employee's compensation, but failure to meet it will decrease the award. Finally, with respect to long-term equity incentive awards, Equifax will no longer grant performance shares tied to three-year cumulative adjusted earnings per share to avoid providing any incentive to limit spending on cybersecurity. The move away from adjusted earnings per share will also alleviate the need to evaluate whether or not to exclude one-time legal expenses when determining long-term incentive compensation, as the remaining long-term performance measures do not contemplate any adjustments.

Ellison Question #7: Shouldn't executives bear the costs of this massive data breach—not just shareholders?

Response: As communicated by Mr. Smith in his testimony, everyone at Equifax is deeply sorry for the cybersecurity incident and apologizes to all of the people whose personal information was potentially impacted. The executives of the Company have felt and will continue to feel the impact of this event in a number of respects. For example, because of the cybersecurity incident, the senior leadership did not receive annual cash incentives with respect to 2017 performance. Aligning the executive's compensation with building long term value for shareholders is good corporate governance and is consistent with this model. The Company's compensation structure reflects that.

Ellison Question #8: How many years has Equifax had a contract with the IRS to verify taxpayers identities, income and employment? Did Equifax also have a contract with the IRS to help combat fraud?

Response: Since 2007, Equifax has been awarded multiple contracts to provide verification and validation services to the IRS. Representative services provided under these contracts include identity and account verification products designed to identify potential identity theft and application fraud.

Ellison Question #9.1: It is my understanding that the short-term \$7.25 million contract awarded to Equifax was a bridge contract because of a contract dispute your former firm had with the IRS. The IRS wanted to bid the contract out to other vendors and Equifax disputed this change. So the bridge contract was to prevent a lapse in service during a protest on another contract. Is that information correct?

Response: On September 29, 2017, Equifax was awarded a bridge contract (task order number TIRNO-17-K-00497 issued against contract number GS00F159DA) to continue providing identification verification and validation services to the IRS while GAO was considering Equifax's protest of the IRS's award of a longer-term contract to provide those services. On October 12, 2017, Equifax received written notice from the IRS to stop work under the subject contract. On October 16, 2017, GAO denied Equifax's bid protest.

Ellison Question #9.2: On what basis did Equifax protest the IRS's action to rebid the contract?

Response: This response was provided in Equifax's 12/29/17 Response Letter to the Committee and is provided here for context.

Equifax's bid protest, which was filed on July 7, 2017, in accordance with 4 C.F.R. § 21.2(a)(2), enumerates Equifax's grounds for submitting the protest to GAO. Equifax protested because it believed IRS's evaluation was inconsistent with the terms of the solicitation. The basis of protest was two-fold. First, Equifax did not believe that Experian could meet the connection requirements described in the solicitation. Second, it appeared that Experian proposed to provide IRS with services that were materially different from the services required by the Solicitation. The protest alleged that IRS's evaluation, which found Experian technically acceptable notwithstanding these issues, was not conducted in accordance with the stated evaluation criteria. On October 16, 2017, GAO denied the bid protest.

Ellison Question #9.3: Does Equifax plan to contest other contracts with other agencies and firms that may be renegotiated following the data breach?

Response: As of the date of this response, Equifax has no such plans.

Ellison Questions ##10–12: Is the data Equifax managed for the IRS encrypted? Is the data in the other databases you manage – TALX, the Work Number, National Consumer Telecom and Utility Exchange, etc. encrypted? Why was the data in your core database not encrypted?

Response: Equifax's core credit reporting database is encrypted; however, that database was not accessed as part of the breach announced on September 7, 2017.

There are a wide range of technologies for protecting data, and encryption is only one method among many. With respect to the incident announced on September 7, 2017, data encryption did not factor into the attackers' ability to access consumer PII. As Mandiant concluded in its executive summary, "the attackers accessed files that contained Equifax credentials (username and password) and performed database queries that provided access to documents and sensitive information stored in databases in an Equifax legacy environment."

For more detailed information about how the attackers accessed consumer information, please see Mandiant's executive summary, supplemental report, and final supplement, which were previously provided to the Committee.

Ellison Question #13: At the hearing you said that the breach was because one employee failed to apply a patch. How much was that one employee paid?

Response: As was discussed in CEO Smith's testimony on October 5, 2017, the criminal attack was made possible by a combination of human error and technological error. The Company will coordinate appropriately with Committee staff regarding the disclosure of private employee information.

Ellison Question #14: It was reported that you [Rick Smith] earned about \$12 million in compensation last year. Is that correct? If not, what was your 2016 compensation? What is the ratio of your compensation to that of your median employee?

Response: For a detailed description of Mr. Smith's 2016 compensation, as well as relevant considerations related to his compensation, please see Equifax's 2017 Proxy Statement, which is available under the Investor Relations section of the Equifax website and is also available through the U.S. Securities and Exchange Commission's (SEC) website.

The ratio of CEO compensation to a company's median employee is a new measure that the SEC has required companies to include beginning in their 2018 Proxy Statements. Along with other public companies, Equifax included the required CEO pay ratio disclosure in its 2018 Proxy Statement, which is available through the Equifax and SEC websites.

Ellison Question #17.3: How many independent contractors does Equifax employ?

Response: As of early November 2017, Equifax employs approximately 5,506 contractors.

Ellison Question #18: In your testimony, you said you had mandated security reviews every quarter. Four meetings a year to protect hundreds of millions of people's personal identification seems inadequate. How big a priority was data security to you as the CEO?

Response: 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.

Ellison Questions ##19 – 24: I am getting many complaints from constituents about your customer service. My constituents say when they call they are on hold for a long time and when they do finally get a response, none of their questions or concerns are answered correctly. How many people have you hired to answer the phones for Equifax? What languages do they speak? What is their average wage? Are they able to join a union? Where are these call centers located? What metrics are you using to measure an appropriate response?

Response: Prior to the September 7, 2017 announcement of the breach, Equifax added approximately 770 incremental call center agents. On September 7, 2017, Equifax added additional call center agents, bringing the total number of incremental call center agents to approximately 1,350. In order to handle the unprecedented call volume following the announcement of the breach, Equifax continued to increase call center staffing. By October 6, 2017, Equifax had added another 2,045 agents to handle authentication and servicing issues, bringing the total number of incremental call center agents to approximately 3,400. Equifax also continuously solicited overtime and double shifts to increase utilization of call center agents. Call center agents can assist consumers in English or in Spanish. Compensation for call center agents varies by location, experience and other issues. Equifax utilized five call centers to handle the call volume relating to the 2017 cybersecurity incident. These included two existing call centers and three additional call centers. Each of the call centers operates in more than one location. These various locations include Nevada, Indiana, Florida, Georgia, Tennessee, Oklahoma, North Dakota, Nicaragua, India, Philippines, and various US-based work from home sites. Call center performance is measured and evaluated based on various standard industry metrics including call volume, wait time, and abandonment rate.

Ellison Questions ##25-27: Following up on Mr. Royce's question on the Bloomberg story, why did Equifax staff tell Fran Rosch at LifeLock about the breach BEFORE Equifax told its government relations staff about the breach? LifeLock is a partner of Equifax, correct? Did Equifax alert LifeLock about the hack so that Equifax's partner could buy "Equifax breach" search terms from google, staff up, prepare products and earn a big profit from the breach?

Response: In April 2016, Equifax partnered with LifeLock to provide data for LifeLock's identity protection services. It is untrue that Equifax earned a large profit from its partnership with LifeLock as a result of the security incident announced on September 7, 2017. For example, from September 7 through December 31, 2017, Equifax earned approximately \$7.7M in revenue from their partnership with LifeLock. During the same period in 2016, Equifax earned approximately \$7.4M.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Denny Heck

Heck Question #5: All states require companies to notify consumers as soon as possible if their information is stolen. Florida requires notification within 30 days. Equifax waited at least 40 days before notifying the public about the breach. How was that delay consistent with the state notification requirements?

Response: Florida's data breach notification statute generally provides that a covered entity shall provide notification of a "breach" or a "breach of security," defined as an unauthorized access of electronic data containing personal information of Florida consumers. (See Fla. Stat. Ann. § 501.171). The statute provides that the notice to impacted Florida consumers "shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or a reason to believe a breach occurred" (See Fla. Stat. Ann. § 501.171(4)(a)).

As contemplated by this statute, Equifax worked diligently with the leading, independent cybersecurity firm, Mandiant, during August and September of 2017 to determine the scope of the incident, including what information was accessed and to identify consumers whose personal information was potentially impacted, in order to make an appropriate public disclosure of the incident. As soon as the Company understood the scope of the incident and the population of consumers whose personal information was potentially impacted, and within 30 days of understanding the scope of the incident and the potentially impacted population, Equifax provided notification to consumers and regulators. By September 4, 2017, Equifax had determined a list of consumers whose personal information was potentially impacted, and on September 7, 2017, the Company provided notification and rolled out a comprehensive support package to consumers.

On September 7, 2017, the Company provided notification of the incident to consumers pursuant to the substitute notification portions of Florida law by issuing a nationwide press release, providing a dedicated incident website with a conspicuous notice on the main Company website, and providing dedicated call centers for consumers. (See Fla. Stat. Ann. § 501.171(4)(f)). The Company also provided written notification to all U.S. State Attorneys General, including the Florida Department of Legal Affairs, Office of the Florida State Attorney General as required under the statute, on September 7, 2017.

Heck Question #7: On what date did Equifax first identify specific records that were accessed in the breach?

Response: In his written testimony to the Committee, then-CEO Rick Smith presented the following timeline:

On August 2, consistent with its security incident response procedures, the company: 1) retained the cybersecurity group at the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; 2) reached out, through company counsel, to engage the independent cybersecurity forensic consulting firm, Mandiant, to investigate the suspicious activity; and 3) contacted the Federal Bureau of Investigation ("FBI").

Over the next several weeks, working literally around the clock, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, how many consumers were affected, and what types of information was accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was not; it had stopped on July 30 when the portal was taken offline). Mandiant also helped examine whether the data accessed contained personal identifying information; discover what data was exfiltrated from the company; and trace that data back to unique consumer information.

By August 11, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables.

On August 15, I was informed that it appeared likely that consumer PII had been stolen. I requested a detailed briefing to determine how the company should proceed.

On August 17, I held a senior leadership team meeting to receive the detailed briefing on the investigation. At that point, the forensic investigation had determined that there were large volumes of consumer data that had been compromised. Learning this information was deeply concerning to me, although the team needed to continue their analysis to understand the scope and specific consumers potentially affected. The company had expert forensic and legal advice, and was mindful of the FBI's need to conduct its criminal investigation.

A substantial complication was that the information stolen from Equifax had been stored in various data tables, so tracing the records back to individual consumers, given the volume of records involved, was extremely time consuming and difficult. To facilitate the forensic effort, I approved the use by the investigative team of

additional computer resources that significantly reduced the time to analyze the data.

Heck Question #8: Of the people who had their information stolen in the hack, how many have been victims of identity theft or payment card fraud, according to Equifax's records?

Response: Equifax has not seen evidence that consumers have experienced identity theft or other financial harm as a result of the cybersecurity incident.

Heck Question #9: Did Equifax initiate any form of credit monitoring of the people affected by the breach at the time it discovered that they were affected or did it wait until after the public notification and then only if the victims signed up for notification?

Response: Equifax issued a nation-wide press release on September 7, 2017 to provide substitute notice to U.S. consumers in accordance with state data breach notification laws. As of that date, U.S. consumers could access the website established by Equifax, www.equifaxsecurity2017.com, to receive further information about the breach, inquire as to whether they may have been impacted, and enroll in TrustedID Premier. Equifax also established a dedicated call center to assist consumers with questions. Per the Fair Credit Reporting Act, the company is prohibited from freezing a consumer report without the consumer's permission.

Heck Question #11: Did Equifax run multiple instances of Apache Struts or run Apache Struts on multiple platforms? If so, was critical vulnerability CVE-2017-5638 successfully patched anywhere within Equifax?

Response: The Company uses multiple instances of Apache Struts, but not all versions were subject to the CVE-2017-5638 Struts vulnerability. The Company has identified and patched all versions of Struts subject to the CVE-2017-5638 Struts vulnerability.

Heck Question #12: If responsibility for patching vulnerabilities is distributed across multiple teams at Equifax, are each of those teams' processes vulnerable to failure if a single employee fails to complete their tasks?

Response: Since discovering the breach, Equifax has improved its patching procedures to require a "closed loop" confirmation that necessary patches have been applied, rolled out a new scanner to identify vulnerabilities, upgraded its security technology, and increased accountability mechanisms for Equifax Security team members.

Heck Question #13: Do Equifax's documented internal risk controls reviewed by management and auditors include descriptions of the process for patching critical vulnerabilities?

Response: Yes. These controls are detailed in the Company's Patch Management Policy. The Company's Patch Management Policy in place in March 2017 categorized patches into four severity groups: critical, high risk, medium risk, and low risk. The policy required that critical patches be applied within 48 hours, high risk patches be applied within 30 days, medium risk be applied within 90 days, and low risk patches be applied within one year of notification. In situations where a patch could not be applied within the given time period, the policy required that Security be consulted and an alternate time period be mutually agreed upon.

Under the policy, following the installation of a critical patch, Security must re-scan within 48 hours to validate that the patch was successful in remediating the vulnerability.

Heck Questions ##15.1 – 15.2: How confident is Equifax that it is not breached now? What gives it confidence?

Response: Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant completed the forensic portion of its investigation of the cybersecurity incident disclosed on September 7 and provided Equifax with an executive summary and final supplemental report, which stated that Mandiant did not identify any evidence of additional or new attacker activity or any access to new databases or tables. For more detailed information about Mandiant's findings and remediation steps, please see the Mandiant executive summary, supplemental report, and final supplement report, all of which were provided to the Committee previously.

Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary. Moreover, Equifax has engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Heck Question #16: Has Equifax shared its cybersecurity lessons learned with the public or any other companies?

Response: Mandiant, a leading independent cybersecurity firm, provided Equifax with an executive summary, a supplemental report, and a final supplement, which collectively detail Mandiant's and Equifax's review process for determining the scope of data exposure for U.S. consumers. Equifax has provided these documents to the Committee, as well as to multiple other Congressional committees and members, federal and state regulators, and business customers. Mandiant's executive summary document described certain initiatives that Equifax realized it needed to take in response to the incident, including:

- Enhancing vulnerability scanning and patch management processes and procedures;
- Reducing the scope of sensitive data retained in backend databases;
- Increasing restrictions and controls for accessing data housed within critical databases;
- Enhancing network segmentation, to restrict access from internet facing systems to backend databases and data stores;
- Deploying additional web application firewalls, and tuning signatures to block attacks;
- Accelerating the deployment of file integrity monitoring technologies on application and web servers;
- Enforcing additional network, application, database, and system-level logging;
- Accelerating the deployment of a privileged account management solution;
- Enhancing visibility for encrypted traffic by deploying additional inline network traffic decryption capabilities;
- Deploying additional endpoint detection and response agent technologies; and
- Deploying additional email protection and monitoring technologies.

Additionally, former Equifax CEOs Rick Smith and Paulino do Rego Barros both testified in public Congressional hearings regarding what they had learned about the breach.

Heck Question #17: Had Equifax previously received information from other companies about lessons they learned from security breaches that they suffered?

Response: Yes, Equifax has historically gathered and shared intelligence about cyber threats and security systems. Equifax collects and shares information with the other national credit bureaus, its financial institution customers, consumer groups, and

government agencies. The company's goal has been to strengthen industry practices and facilitate stronger standards for cybersecurity programs. Equifax is committed to improving industry standards to benefit the marketplace including consumers, credit bureaus and financial institutions.

Heck Question #19: News reports indicate that Equifax had suffered a breach in March for which it brought in a third party cybersecurity firm. On how many occasions this year prior to July 29 had Equifax hired a third party to assist with cybersecurity or investigate a breach? On how many occasions in the two years leading up to July 29?

Response: Please note that Equifax and its subsidiaries have never before experienced an intrusion involving U.S. consumer PII of the type and scale announced on September 7, 2017. The incident mentioned in news reports involved the Tax Form Management service of Equifax subsidiary TALX Corporation. One or more bad actors appear to have used PII previously obtained from unknown sources to fraudulently pass knowledge-based authentication processes and access the Form W-2 information of certain employees of some of TALX's employer-customers, as well as a few Paperless Pay accounts of one employer-customer. This TALX account-takeover incident was the one time last year, prior to July 29, that Equifax hired outside counsel and worked with third-party forensic consultants to assist with investigating an incident that involved the unauthorized access to or acquisition of U.S. consumer PII by one or more bad actors.

During 2015 and 2016, there were three other incidents when Equifax hired outside counsel to assist with the investigation, one of which also involved working with a third-party forensic consultant firm.

Heck Question #20: Was the information that was stolen encrypted by any method?

Response: There are a wide range of technologies for protecting data, and encryption is only one method among many. With respect to the incident announced on September 7, 2017, data encryption did not factor into the attackers' ability to access consumer PII. As Mandiant concluded in its executive summary, "the attackers accessed files that contained Equifax credentials (username and password) and performed database queries that provided access to documents and sensitive information stored in databases in an Equifax legacy environment."

For more detailed information about how the attackers accessed consumer information, please see Mandiant's executive summary, which was provided to the Committee previously.

Equifax's core credit reporting database is encrypted; however, that database was not accessed as part of the breach announced on September 7, 2017. Please see response to Ellison questions #10-12.

Heck Question #21: Was Equifax compliant with Payment Card Industry Data Security Standards for encryption?

Response: Data security and integrity are of paramount importance to Equifax, and Equifax was PCI-certified prior to the incident announced on September 7, 2017. The systems at issue in the incident, however, were located outside of the PCI environment maintained by Equifax.

There are a wide range of technologies for protecting data, and encryption is only one method among many. Data encryption alone would not have prevented the incident announced on September 7, 2017. As Mandiant concluded in its executive summary, “the attackers accessed files that contained Equifax credentials (username and password) and performed database queries that provided access to documents and sensitive information stored in databases in an Equifax legacy environment.”

For more detailed information about how the attackers accessed consumer information, please see Mandiant’s executive summary, which was previously provided to the Committee.

Heck Question #22: What federal regulations on data encryption is Equifax subject to?

Response: Equifax is not subject to any federal regulation on encryption. Equifax does comply with or maintain certifications in different areas of the business that mandate the encryption of data at rest and in transit. For example, some business units have a FISMA certification while other parts of the Company have a PCI certification. In order to maintain standardization across these different certifications with regards to encryption, Equifax, as stated in its Cryptography Standard, mandates the use of FIPS 140-2 compliant algorithms. To that end, Equifax requires the use of the AES encryption algorithm. For data at rest, Equifax utilizes AES-256bit encryption. For data in transit, Equifax mandates the use of AES-128bit encryption. The use of FIPS-104-2 compliant algorithms for the protection of sensitive data is mandated by NIST.

Heck Question #24: Was the timeline for internally notifying executives identical to the process in earlier breaches?

Response: The process and timeline for informing the Chief Security Officer, the Chief Legal Officer, the Chief Executive Officer and other senior leaders regarding a cybersecurity incident varied depending upon the severity of the incident. Equifax never before experienced a data security incident approaching the magnitude of the incident announced September 7, 2017.

Heck Question #27: Has Equifax ever blocked stock sales during a prior investigation of a security breach?

Response: The special trading blackout initiated in August 2017 was the first such trading restriction imposed as a result of a cybersecurity incident.

Heck Question #28: Former CEO Richard Smith testified that his retirement package reported in the press was all pension and stock that he had already earned. Were all of those shares of stock vested before he announced his retirement? If not, who made the decision to allow him to keep unvested stock while departing the company? How many shares of stock were unvested before his retirement announcement?

Response: As previously disclosed, Richard Smith retired from Equifax on September 26, 2017. However, all decisions related to the characterization of Mr. Smith's departure and any benefits owed to him were deferred to allow the Board of Directors to complete an independent review of matters relating to the 2017 cybersecurity incident. The Compensation Committee of the Board, advised by independent counsel, completed its review and determined that Mr. Smith is entitled to receive equity previously awarded to him pursuant to the Company's 2008 Omnibus Incentive Plan, and that he has retired from Equifax under the terms of the governing award agreements. Consequently, the shares that he would have been entitled to receive upon vesting in February 2018 and that were placed in escrow have been released.

Heck Question #29: Washington state law prohibits credit reporting agencies from releasing a credit report for an account under a credit freeze except in the case that the requestor has authorization from the person whose file is being requested or for certain government functions. Are there any differences between when a credit report could be released for an file under Equifax's announced "credit lock" and when it can be released under Washington's credit freeze law? What are those differences?

Response: At the most basic level, a credit report lock and a security freeze both generally prevent unauthorized access to a consumer's credit report to open new credit 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 report lock in place. With the passage of S.2155, which was signed into law on May 24, 2018, credit freezes will now be regulated by federal law and will be free to all consumers.

Security freezes (also known as credit freezes) use a PIN-based system for authentication. Credit report locks are mobile-enabled and use usernames and passwords for authentication.

Detailed directions for freezing or locking an Equifax credit report are set forth on the company's website.

On January 31, 2018, Equifax announced the availability of Lock & Alert, a new service that enables consumers to quickly lock and unlock their Equifax credit report using a computer or app downloaded on their mobile device. Lock & Alert is available for free, for life.

Heck Question #30: Equifax had a contract with the IRS to provide knowledge-based authentication of users for certain IRS online services. Has any of the information obtained by hackers been part of the information tested in the knowledge-based authentication question on the IRS or other sites? If so, have authentication questions using that information been removed? If so, when were those questions removed?

Response: Equifax's service provided to the IRS for online identify verification comprised of a risk-based authentication platform, not a knowledge-based authentication protocol. Equifax utilized the knowledge-based authentication protocols for identity verification services in IRS call centers. These protocols required a caller to provide accurate answers to several multiple-choice, dynamically-generated questions that included information from Equifax's core consumer reporting databases—none of which were impacted by the recent security incident—such as a consumer's current and past employers, previously closed loans, and certain utilities account information. Because the attackers did not access the core consumer credit database, they did not steal sufficient information to successfully answer knowledge-based authentication questions. Equifax remains fully confident in this service and the value it provided to the IRS.

Heck Question #31: Has anyone contacted Equifax claiming to be the hacker? Has that claim been validated?

Response: 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.

Heck Question #32: In my opinion, the absolute bare minimum Equifax owes to the people affected by the breach is: 1) Reaching out to notify everyone whose information was disclosed in the breach; 2) Providing free credit monitoring for the lifetime of those affected; 3) Covering the cost of credit freezes at Equifax and the other major credit bureaus for those who want them. Will you commit to notifying all of those affected and covering their costs for notification and freezes at all three bureaus?

Response: Equifax has taken steps to notify consumers and provide them with a variety of tools. Recognizing that consumers rely on access to credit, Mandiant, a leading independent cybersecurity firm, was engaged to investigate the scope of the incident. Mandiant provided Equifax with an executive summary, a supplemental report, and a final supplement, which collectively detail Mandiant's and Equifax's review process for determining the scope of impacted information for U.S. consumers. Equifax has provided these documents to the Committee previously.

Equifax has notified consumers potentially impacted by this incident consistent with state data breach notification laws. On September 7, 2017, Equifax provided notification of the incident by issuing a nationwide press release, providing a dedicated website where consumers could determine if their personal information was potentially impacted and, regardless of whether or not their personal information was potentially impacted, sign up for a free credit file monitoring and identity theft protection product, and by providing a dedicated call center for consumers to obtain more information. The notification indicated that the incident impacted personal information relating to approximately 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.

Equifax provided notification pursuant to the state data breach notification statutes that impose various notice requirements and allow companies to provide notification through various methods to meet those requirements. Equifax's notification included both substitute notification (as contemplated by the state data breach statutes using a nationwide press release, dedicated website, and call center), and through direct mail notification for certain groups of potentially impacted consumers. Specifically, Equifax mailed written notices to consumers whose credit card numbers or dispute documents were impacted, as well as to the approximately 2.5 million additional U.S. consumers whose personal information was potentially impacted identified since the September 7, 2017 announcement and notification.

Equifax also has posted and updated FAQs on the www.equifaxsecurity2017.com website in recent months, addressing questions we have received from consumers. More information about credit and identity theft protection is available on www.equifaxsecurity2017.com, through the Lock & Alert service online, within the Lock & Alert mobile app, and on Equifax's YouTube channel.

Finally, with the passage of S.2155, which was signed into law on May 24, 2018, credit freezes will now be regulated by federal law and will be free to all consumers.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Brad Sherman

Sherman Question #1: How much have you made – pensions, stock options, and salary – from Equifax during your time with the company?

Response: For a detailed description of Mr. Smith's compensation during his time with Equifax, as well as relevant considerations related to his compensation, please see Equifax's Proxy Statements, starting with the 2006 statement, which are available under the Investor Relations section of the Equifax website and are also available through the U.S. Securities and Exchange Commission's website.

Sherman Question #2: My home state of California has very specific notification requirements when a data breach exposes personally identifiable information. Has Equifax complied with any state laws or regulations that require the company to notify specific individuals who have had their data exposed in this breach?

Response: Equifax complied with all state data breach notification requirements. 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.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Kyrsten Sinema

Sinema Question #1: You mentioned that Equifax is a frequent target of cyber attacks. On average, how many attempted attacks does Equifax experience on a daily and monthly basis?

Response: As Mr. Smith testified, there are millions of attempted or suspicious attacks each and every year, across a wide array of Equifax's data assets. Equifax's Cyber Threat Center logs hundreds of thousands of potential security events on a weekly basis.

Because Equifax's products and services involve the storage and transmission of personal information of consumers, Equifax continues to routinely be the target of attempted cyber and other security threats by outside third parties, including technically sophisticated and well-resourced bad actors attempting to access or steal the data Equifax stores. In addition, the 2017 cybersecurity incident may embolden individuals or groups to target Equifax's systems. Equifax continuously monitors and develops its information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact.

Sinema Questions ##2-3: The attack vectors for these attempted breaches are numerous and frequent. Can you provide additional perspective on how Equifax adapts its systems to mitigate these attempts? Can you provide insight on why you think it failed in this case? What changes has Equifax made to the IT department that failed to address the Apache Struts vulnerability? In addition to detailing any staff that were fired as a result, please provide a list of changes to company best practices to ensure that software patches are installed in the prescribed timeframe.

Response: The breach occurred because of both human error and technology failures. These mistakes were made in the same chain of security systems designed with redundancies.

Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level

logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Importantly, Equifax's forensic consultants have recommended a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax has also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the Company since September 7, 2017. Equifax also has appointed Mark Begor as the company's new CEO and Jamil Farshchi as the company's new Chief Information Security Officer.

Sinema Question #4: What have you learned from this incident that can be used to prevent and address future data breaches in both the public and private sector?

Response: Equifax has hosted and participated in numerous briefings with government regulators and industry stakeholders to discuss the incident that was announced on September 7, 2017. Equifax has focused on both short term remediation activities and long term strategic transformation to ensure that its cybersecurity program provides Equifax's customers and consumers with strong protections. Equifax is also committed to ensuring the Company is well-equipped to prevent, detect, and respond to cybersecurity incidents.

* * *

