

# OVERSIGHT OF THE EQUIFAX DATA BREACH: ANSWERS FOR CONSUMERS

---

## HEARING BEFORE THE SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 3, 2017

**Serial No. 115–59**



Printed for the use of the Committee on Energy and Commerce  
*energycommerce.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

27–462

WASHINGTON : 2019

## COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon  
*Chairman*

JOE BARTON, Texas <i>Vice Chairman</i>	FRANK PALLONE, JR., New Jersey <i>Ranking Member</i>
FRED UPTON, Michigan	BOBBY L. RUSH, Illinois
JOHN SHIMKUS, Illinois	ANNA G. ESHOO, California
TIM MURPHY, Pennsylvania	ELIOT L. ENGEL, New York
MICHAEL C. BURGESS, Texas	GENE GREEN, Texas
MARSHA BLACKBURN, Tennessee	DIANA DEGETTE, Colorado
STEVE SCALISE, Louisiana	MICHAEL F. DOYLE, Pennsylvania
ROBERT E. LATTA, Ohio	JANICE D. SCHAKOWSKY, Illinois
CATHY McMORRIS RODGERS, Washington	G.K. BUTTERFIELD, North Carolina
GREGG HARPER, Mississippi	DORIS O. MATSUI, California
LEONARD LANCE, New Jersey	KATHY CASTOR, Florida
BRETT GUTHRIE, Kentucky	JOHN P. SARBANES, Maryland
PETE OLSON, Texas	JERRY McNERNEY, California
DAVID B. MCKINLEY, West Virginia	PETER WELCH, Vermont
ADAM KINZINGER, Illinois	BEN RAY LUJAN, New Mexico
H. MORGAN GRIFFITH, Virginia	PAUL TONKO, New York
GUS M. BILIRAKIS, Florida	YVETTE D. CLARKE, New York
BILL JOHNSON, Ohio	DAVID LOEBSACK, Iowa
BILLY LONG, Missouri	KURT SCHRADER, Oregon
LARRY BUCSHON, Indiana	JOSEPH P. KENNEDY, III, Massachusetts
BILL FLORES, Texas	TONY CARDENAS, California
SUSAN W. BROOKS, Indiana	RAUL RUIZ, California
MARKWAYNE MULLIN, Oklahoma	SCOTT H. PETERS, California
RICHARD HUDSON, North Carolina	DEBBIE DINGELL, Michigan
CHRIS COLLINS, New York	
KEVIN CRAMER, North Dakota	
TIM WALBERG, Michigan	
MIMI WALTERS, California	
RYAN A. COSTELLO, Pennsylvania	
EARL L. "BUDDY" CARTER, Georgia	

## SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION

ROBERT E. LATTA, Ohio  
*Chairman*

GREGG HARPER, Mississippi <i>Vice Chairman</i>	JANICE D. SCHAKOWSKY, Illinois <i>Ranking Member</i>
FRED UPTON, Michigan	BEN RAY LUJAN, New Mexico
MICHAEL C. BURGESS, Texas	YVETTE D. CLARKE, New York
LEONARD LANCE, New Jersey	TONY CARDENAS, California
BRETT GUTHRIE, Kentucky	DEBBIE DINGELL, Michigan
DAVID B. MCKINLEY, West Virginia	DORIS O. MATSUI, California
ADAM KINZINGER, Illinois	PETER WELCH, Vermont
GUS M. BILIRAKIS, Florida	JOSEPH P. KENNEDY, III, Massachusetts
LARRY BUCSHON, Indiana	GENE GREEN, Texas
MARKWAYNE MULLIN, Oklahoma	FRANK PALLONE, JR., New Jersey ( <i>ex officio</i> )
MIMI WALTERS, California	
RYAN A. COSTELLO, Pennsylvania	
GREG WALDEN, Oregon ( <i>ex officio</i> )	

## CONTENTS

---

	Page
Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, opening statement .....	2
Prepared statement .....	3
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement .....	4
Hon. Greg Walden, a Representative in Congress from the State of Oregon, prepared statement .....	5
Prepared statement .....	7
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, prepared statement .....	8
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, prepared statement .....	67
WITNESSES	
Richard Smith, Former Chairman and CEO of Equifax, Inc. ....	10
Prepared statement .....	12
Answers to submitted questions <sup>1</sup> .....	74
SUBMITTED MATERIAL	
Statement of consumer groups .....	69
Statement of the Credit Union National Association .....	71
Article entitled, “Equifax investigating stock sales made by executives during data breach,” CNN Wire, October 1, 2017 .....	72

---

<sup>1</sup> The committee did not receive a response to Mr. Smith’s submitted questions for the record by the time of printing.



## **OVERSIGHT OF THE EQUIFAX DATA BREACH: ANSWERS FOR CONSUMERS**

**TUESDAY, OCTOBER 3, 2017**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER  
PROTECTION,  
COMMITTEE ON ENERGY AND COMMERCE,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:00 a.m., in room 2123 Rayburn House Office Building, Hon. Robert Latta (chairman of the subcommittee) presiding.

Members present: Representatives Latta, Harper, Burgess, Upton, Lance, Guthrie, McKinley, Kinzinger, Bilirakis, Bucshon, Mullin, Walters, Costello, Walden (ex officio), Schakowsky, Luján, Clarke, Cárdenas, Dingell, Matsui, Welch, Kennedy, Green, and Pallone (ex officio).

Also present: Representatives Barton, Murphy, Carter, Degette, Tonko, and McNerney.

Staff present: Jennifer Barblan, Chief Counsel, Oversight & Investigations; Ray Baum, Staff Director; Karen Christian, General Counsel; Kelly Collins, Staff Assistant; Zachary Dareshori, Staff Assistant; Jordan Davis, Director of Policy and External Affairs; Melissa Froelich, Chief Counsel, Digital Commerce and Consumer Protection; Adam Fromm, Director of Outreach and Coalitions; Ali Fulling, Legislative Clerk, Oversight & Investigations, Digital Commerce and Consumer Protection; Theresa Gambo, Human Resources/Office Administrator; Elena Hernandez, Press Secretary; Zach Hunter, Director of Communications; Bijan Koohmaraie, Counsel, Digital Commerce and Consumer Protection; Alex Miller, Video Production Aide and Press Assistant; Mark Ratner, Policy Coordinator; Dan Schneider, Press Secretary; Sam Spector, Policy Coordinator, Oversight & Investigations; Madeline Vey, Policy Coordinator, Digital Commerce and Consumer Protection; Hamlin Wade, Special Advisor, External Affairs; Jessica Wilkerson, Professional Staff, Oversight & Investigations; Everett Winnick, Director of Information Technology; Greg Zerzan, Counsel, Digital Commerce and Consumer Protection; Michelle Ash, Minority Chief Counsel, Digital Commerce and Consumer Protection; Priscilla Barbour, Minority Energy Fellow; Jean Fruci, Minority Energy and Environment Policy Advisor; Rick Kessler, Minority Senior Advisor and Staff Director, Energy and Environment; Alexander Ratner, Minority Policy Analyst; and Tuley Wright, Minority Energy and Environment Policy Advisor.

**OPENING STATEMENT OF HON. ROBERT E. LATTA, A  
REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO**

Mr. LATTA. Good morning. The subcommittee on Digital Commerce and Consumer Protection will come to order. The chair now recognizes himself for 5 minutes for an opening statement.

Good morning. Today we are here to get the facts to learn what happened at Equifax that led to the personal information of over 143 million Americans' information being stolen. Americans need to know what Equifax is doing to fix the problem and help individuals that are impacted. We must find out what happened. The public deserves to know what happened and what steps are being taken to protect their sensitive data going forward.

Today's hearing needs to shed some much needed information and light on this breach. We have received assurances from Equifax that Mr. Smith can speak for the company on concrete remediation steps that the company took in the aftermath to secure its computer systems to protect the affected U.S. customers as well as what happened when he was chief executive.

As chairman of the Digital Commerce and Consumer Protection subcommittee, I often speak about the fact that we live in a digitally-connected world. That fact of life can have many positive implications, far and wide-ranging, for commerce, trade, communications, and entertainment. The breach is a massive reminder of the bad actors that are out there and the security challenges confronting our digitally integrated and data-powered economy.

In this case, sensitive personal information that is used to build credit histories and allow individuals to engage in commerce, open credit cards, buy cell phones and appliances, and secure mortgages has been compromised. Reasonable security measures must be implemented, practiced, and continually improved by companies that collect and store data in order to guard against unauthorized access to sensitive personal information. Otherwise, consumers will face substantial financial harm.

This risk is deeply concerning to me and I know that the other members of the subcommittee share this view. Priority number one: We must protect Americans and work to safeguard their personal information online. The recent Equifax data breach is unprecedented and is also unique because of the sensitivity of the information stolen, including full nine-digit Social Security numbers.

Over 143 million Americans are potentially impacted. This represents approximately 44 percent of the total U.S. population. In my home State of Ohio, approximately 5.2 million customers are likely affected. Based on the information released by Equifax, we are informed that the massive amounts of personal and financial information was assessed from mid-May through July 2017, including names, birthdates, addresses, and in some cases driver's license information. In addition, over 200,000 people had their credit card information stolen and over 180,000 people had credit dispute documentation stolen.

This is a staggering amount of sensitive personal information and impacts an extraordinary number of credit-visible Americans that is in the hands of criminals that could result in fraud or identity theft. We need these numbers confirmed. Today, we must understand the following:

First, how did the hackers get into Equifax's system for so many weeks and pull so much information out of the system without being detected?

Second, what processes and procedures were in place in the event of such a breach and were those processes followed? There are many questions as to who knew what and when this information was known. This will have implications in other ongoing investigations. Further, the chief information officer and chief security officer made retirement announcements shortly after the public notice of the breach and have not been available for questions about their role.

Again, despite months of delay, why was Equifax's notification and consumer protection process still met with misinformation, glitches, and overall confusion? For example, there were numerous reports of difficulties accessing Equifax's dedicated web site or call centers. And there were dismaying reports that the official Equifax Twitter account directed consumers to a fake web site.

I believe the American public deserves to know the facts about when and how Mr. Smith, company management, and the board of directors were made aware its systems were vulnerable to hackers and how over 143 million sensitive personal data records were stolen. To that end, what were the steps taken and in what timeframe to notify and help individuals that were impacted? I look forward to getting these answers today and many more questions for the American people answered this morning.

And at this time I will ask the gentlelady from Illinois, the ranking minority member, for 5 minutes for her opening statement.

[The prepared statement of Mr. Latta follows:]

#### PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good morning, today we are here to get the facts to learn what happened at Equifax that led to the personal information of over 143 million Americans being stolen. Americans deserve to know what Equifax is doing to fix the problems and help individuals that are impacted. We must find out what happened.

The public deserves to know what happened and what steps are being taken to protect their sensitive data going forward.

Today's hearing needs to shed some much needed light on this breach. We have received assurances from Equifax that Mr. Smith can speak for the company on concrete remediation steps the company took in the aftermath to secure its computer systems and to protect affected U.S. consumers, as well as what happened when he was the Chief Executive.

As Chairman of the Digital Commerce and Consumer Protection Subcommittee, I often speak about the fact that we live in a digitally-connected world. That fact of life can have many positive implications, far and wideranging, for commerce, trade, communications and entertainment.

This Equifax breach is a massive reminder of the bad actors that exist and of the security challenges confronting our digitally-integrated and data-powered economy. In this case, sensitive personal information that is used to build credit histories and allow individuals to engage in commerce-open credit cards, buy cell phones and appliances, and secure mortgages has been compromised.

Reasonable security measures must be implemented, practiced, and continually improved by companies that collect and store data in order to guard against unauthorized access to sensitive personal information. Otherwise, consumers can face substantial financial harm. This risk is deeply concerning to me, and I know the other Members of this Subcommittee share that view.

Priority number one: We must protect Americans and work to safeguard their personal information online.

The recent Equifax data breach is unprecedented and it is also unique because of the sensitivity of information stolen- including full nine-digit social security num-

bers. Over 143 million Americans are potentially impacted. This represents approximately 44% of the total U.S. population. In my home State of Ohio, approximately 5.2 million consumers are likely affected.

Based on the information released by Equifax, we are informed that the massive amounts of personal and financial information was accessed from mid-May through July 2017, including names, birthdates, addresses, and in some cases, driver's license information. In addition, over 200,000 people had their credit card information stolen, and over 180,000 people had credit dispute documentation stolen.

That is a staggering amount of sensitive personal information. It impacts an extraordinary number of creditvisible Americans, that in the hands of bad actors that could result in fraud or identity theft. We need these numbers confirmed.

Today, we must understand the following:

First, how did the hackers get into Equifax's system for so many weeks and pull so much information out of the system without being detected?

Second, what processes and procedures were in place in the event of such a breach and were those processes followed? There are many questions as to who knew what, and when this information was known? This will have implications in other ongoing investigations. Further, the Chief Information Officer and Chief Security Officer made retirement announcements shortly after the public notice of the breach and have not been available for questions about their role.

And, despite months of delay, why was Equifax's notification and consumer protection process still met with misinformation, glitches, and overall confusion? For example, there were numerous reports of difficulties accessing Equifax's dedicated web site or call centers. And there were dismaying reports that the official Equifax Twitter account directed consumers to a fake web site.

I think the American public deserves to know the facts about when and how Mr. Smith, company management, and the board of directors were made aware its systems were vulnerable to hackers and over 143 million sensitive personal data records were stolen. Then, what were the steps taken and in what timeframe to notify and help individuals that were impacted.

I look forward to getting answers to these and many more questions for the American public this morning.

#### **OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS**

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, for holding this hearing. The Equifax data breach was massive in scale: 145.5 million American victims as of yesterday. I would call it shocking, but is it really? We have these underregulated, private, for-profit credit reporting agencies collecting detailed personal and financial information about American consumers. It is a treasure trove for hackers.

Consumers don't have a choice over what information Equifax or, for example, TransUnion, or Experian have collected, stored, and sold. If you want to participate in today's modern economy, if you want to get a credit card, rent an apartment, or even get a job, often then a credit reporting agency may hold the key.

Because consumers don't have a choice, we can't trust credit reporting agencies to self-regulate. It is not like when you get sick at a restaurant and decide not to go there anymore. Equifax collects your data whether you want to have it collected or not. If it has incorrect information it is really an arduous process—I have tried it—to get it corrected. When it comes to information security you are at the mercy of whatever Equifax decides is right and once your information is compromised the damage is ongoing.

Given vast quantities of information and lack of accountability, a major breach at Equifax I would say would be predictable if not inevitable. I should really say breaches. This is the third major breach Equifax has had in the past 2 years. From media reports



and the subcommittee's meeting with Equifax officials after the breach, it is clear to me that the company lacked appropriate policies and practices around data security.

This particular breach occurred when hackers exploited a known vulnerability that was not yet patched. It was months later before Equifax first discovered the breach, and it was another several weeks before Equifax shared news with the consumers, this committee, the Federal Trade Commission, and the Consumer Financial Protection Bureau.

Senior officials at the company are saying they weren't immediately aware that the breach occurred, and yet by the way there were executives who sold over a million dollars in stock just before, days after the breach was discovered but yet not reported. And for a lot of Americans that just doesn't pass the smell test.

The response to the breach was its own debacle. Equifax offered consumers credit monitoring services that initially came with a mandatory arbitration clause which fortunately has been corrected; Equifax tweeted links to the wrong URL directing victims to a fake web site; the call center was understaffed; and in the end Equifax has had to apologize for its supposed breach response almost as much as it has apologized for the breach itself.

Equifax deserves to be shamed in this hearing, but we should also ask what Congress has done or failed to do to stop data breaches from occurring and what Equifax plans to do. The same day the Equifax breach went public the House Financial Services Committee held a hearing on FCRA Liability Harmonization Act, a bill to protect credit reporting agencies like Equifax from class action suits. Imagine.

In fact, Equifax was lobbying for this bill after the breach was discovered in July, still not reported, and the 14 Republicans sponsoring this bill should ask themselves whether this is really the industry they want to be in bed with. Companies like Equifax need more accountability, not less. I agree with the CFPB director Richard Cordray that the credit reporting agencies need embedded regulators to protect consumers' sensitive information.

And then we need to go further. Last night, I reintroduced the Secure and Protect Americans' Data Act, along with Ranking Member Pallone and seven other members of the Energy and Commerce Committee. And our bill would establish, one, strong data security standards; two, require prompt breach notification, which we didn't get; and three, provide appropriate relief for breached victims.

Chairman Latta, American consumers don't just need answers, they need action. I hope that our bill can be a starting point for discussion on strengthening protections for Americans' data. Consumers deserve a whole lot better than they got from Equifax. And I yield back.

Mr. LATTA. Thank you very much. The gentlelady yields back. The chair now recognizes the gentleman from Oregon, the chairman of the full committee, for 5 minutes.

**OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON**

Mr. WALDEN. I thank the chairman. We are here to do today what it appears Equifax failed to do over the last several months

and that is put consumers first. Our job is to get answers for the more than 145 million Americans who have had their personal information compromised and now fear they could be victims of fraud at any time.

How could a major U.S. company like Equifax, which holds the most sensitive and personal data on Americans so let them down? It is like the guards at Fort Knox forgot to lock the doors and failed to notice the thieves were emptying the vaults. The American people deserve to know what went wrong. We want a clear timeline of events and to understand what to expect moving forward.

Mr. Chairman, the Energy and Commerce Committee has always tried to put our consumers first in everything we do on public policy. So today we will begin to get the answers for the public, hold Equifax accountable, and make clear that businesses holding America's most sensitive data have a responsibility under existing laws to protect that data. Today gives whole new meaning to Mr. Smith Goes to Washington. It is not a run on the bank that is at issue, it is a run on financial records of 145 million Americans. And the consequences and the inconveniences for our fellow citizens is every bit as important to discuss today as the reasons behind why this breach occurred in the first place.

Mr. Smith, as former chairman and CEO of Equifax at the helm during and immediately after the breach, we appreciate you being here and we expect your candor and full cooperation as we march toward getting the facts in this case. While there is no such thing as perfect security, companies do have a legal obligation to protect sensitive consumer data. This diligence is necessary to both comply with existing laws and maybe more importantly earn and keep the public's trust in a data-driven economy.

Given the size of the breach and the sensitivity of the data, we expect to learn more about how Equifax failed to secure its systems and what contingency plans were in place. Further, we need to understand how information flowed through the organization and when you and other senior executives were notified about the breach. In other words, how important was cybersecurity to you as a CEO and to the rest of your executive team? Did your employees have a way to report to you if they had concerns about how the security team was functioning?

While there are still many questions that need answers, a few details have emerged. First, the vulnerability that the hackers used to get into the Equifax system was discovered in early March. From the beginning, the vulnerability was described as critical and easily exploitable. That information was pushed out through multiple security information sharing channels including by the U.S. Computer Emergency Readiness Team to Equifax's chief security officer.

For some period of time between March and August of 2017, the hackers were able to sit on Equifax's system and siphon out 145 million records without being detected. How did this go unnoticed? Further, is there a process in place to raise flags or alarms when massive amounts of data are pulled out of the Equifax system?

Then there are questions about Equifax's response for consumers that we need answers to. Why was the consumer-facing web site created on a separate domain from the main Equifax web site? Did

anyone raise concerns about creating more consumer confusion with a separate web site? Are consumers able to sign up for the products offered by Equifax today? How many consumers have placed a fraud alert on their account or frozen their credit?

And on top of all the other issues, multiple times Equifax tweeted the wrong URL directing consumers to the wrong web site to check if they were part of a breach. Talk about ham-handed responses, this is simply unacceptable and it makes me wonder whether there was a breach response plan in place at all and if anyone was in charge of overseeing and executing that plan. I have to agree with the interim CEO when he said there is insufficient support for consumers.

It is important that as Congress does its work on public policy issues that the Federal Trade Commission and other agencies, including law enforcement agencies, continue their work especially in light of recent reports that indicated there are markers of nation state activity involved with this hack. But today, Mr. Smith, I and the rest of the committee and Congress and the country expect the answers. After all, the buck does stop with you as CEO and I thank you for being here. And I return the balance of my time.

[The prepared statement of Mr. Walden follows:]

#### PREPARED STATEMENT OF HON. GREG WALDEN

We are here today to do what it appears Equifax failed to do over the last several months: put consumers first. Our job is to get answers for the more than 145 million Americans who have had their personal information compromised and now fear that they could be victims of fraud at any time.

How could a major U.S. company like Equifax, which holds the most sensitive and personal data on Americans, so let them down? It's like the guards at Fort Knox forgot to lock the doors and failed to notice thieves emptying the vaults.

The American people deserve to know what went wrong. We want a clear timeline of events, and to understand what to expect moving forward.

As Chairman of the Energy and Commerce Committee, I've tried to put consumers at the forefront of everything we do. Today we will begin to get answers for the public, hold Equifax accountable, and make clear that businesses holding Americans' sensitive information have a responsibility under existing laws to protect those data.

Today gives whole new meaning to Mr. Smith Goes to Washington. It's not a run on the bank at issue, it's a run on the financial records of 145 million Americans. The consequence and inconveniences for our fellow citizens is every bit as important to discuss today as the reasons behind why this breach occurred in the first place.

Richard Smith, the former Chairman and CEO of Equifax at the helm during and immediately after the breach, is here to testify. Mr. Smith, we expect your candor and full cooperation as we follow the facts in this case.

While there is no such thing as perfect security, companies do have a legal obligation to protect sensitive consumer data. This diligence is necessary to both comply with existing law and, maybe more importantly, earn and keep the public's trust in our data driven economy.

Given the size of the breach and the sensitivity of the data, we expect to learn more about how Equifax failed to secure its systems and what contingency plans were in place.

Further, we need to understand how information flowed through the organization and when you and other senior executives were notified about the breach. In other words, how important was cybersecurity to you as CEO and to the rest of your executive team? Did your employees have a way to report to you if they had concerns about how the security team was functioning?

While there are still many questions that need answers, a few details have emerged. First, the vulnerability that the hackers used to get into the Equifax system was discovered in early March. From the beginning, the vulnerability was described as critical and easily exploitable. That information was pushed out through

multiple security information sharing channels, including by the U.S. Computer Emergency Readiness Team, to Equifax's Chief Security Officer.

For some period of time between March and August 2017, the hackers were able to sit on Equifax's system and siphon out 145 million records without being detected. How did this go unnoticed? Further, is there a process in place to raise flags or alarms when massive amounts of data are pulled out of the Equifax system?

Then there are the questions about Equifax's response for consumers.

- Why was the consumer-facing web site created on a separate domain from the main Equifax web site?
- Did anyone raise concerns about creating more consumer confusion with a separate web site?
- Are consumers able to sign up for the products offered by Equifax today?
- How many consumers have placed a fraud alert on their account or frozen their credit?

On top of all of the other issues, multiple times Equifax tweeted the wrong URL directing consumers to the wrong web site to check if they were a part of the breach. Talk about ham-handed responses. This is unacceptable. And it makes me wonder whether there was a breach response plan in place, and if anyone was in charge of overseeing and executing that plan.

I have to agree with the interim CEO, there is "insufficient support for consumers." It's important that as Congress does its work on public policy issues, that the Federal Trade Commission and law enforcement agencies continue with their work, especially in light of recent reports that indicated there are markers of nation-state activity.

But today, Mr. Smith, I, the rest of this committee, Congress, and the country expect answers. After all, the buck stops with you, as CEO.

Mr. LATTA. Thank you very much. The gentleman yields back and the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee. Good morning.

**OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY**

Mr. PALLONE. Thank you, Mr. Chairman. While I understand that law enforcement and internal investigations into this incident are still ongoing, I expect to get more information today on what happened and why it took so long to inform the public. Most importantly, we want answers for consumers because Equifax's response to this breach has been unacceptable. So too has been Equifax's ongoing lax attitude when it comes to protecting consumer data.

It has been 4 weeks since the breach was made public and at least 10 weeks since it was discovered by Equifax's employees, yet Equifax's customer service has been confusing and unhelpful. Equifax even tweeted a link to a fake web site. Many of the remedies Equifax is now offering to consumers were not offered upfront or in good faith. They were forced out of the company only after a public outcry and they are still inadequate.

It is hard to imagine that anyone at Equifax thought it was a good idea to offer only 1 year of credit monitoring, with an arbitration clause at first to boot. Free and comprehensive credit monitoring and identity theft protection should be offered for far longer than a year. Most recently, Equifax added lifetime credit locks to its offering which consumer advocates suggest are weaker than credit freezes. Regardless, a lock or a freeze at only one credit bureau is almost useless. Equifax should work with the other credit bureaus to immediately create a free, quick, and easy-to-use freeze and unfreeze one-stop shop.

And because credit freezes or locks may not work for everyone, going forward Equifax should do more than credit locks. It should give consumers more control over how their data is used and stored. In addition, if Equifax wants to stay in business, its entire corporate culture needs to change to one that values security and transparency. After all, this is not Equifax's first data breach in the past year.

Consumers do not have any say in whether or not Equifax collects and shares their data and that is what makes this breach so concerning. This is unlike other breaches at stores such as Target and Michael's where consumers could make a choice and change their shopping habits if they were upset with how the companies protected data. That is simply not the case with Equifax.

While data breaches have unfortunately become commonplace, it is long past time for Congress, beginning with this committee, to act. Since at least 2005, this subcommittee has been considering data breach legislation but it has never become law and it is time we changed that. Yesterday, Ranking Member Schakowsky and I reintroduced the Secure and Protect Americans' Data Act. This bill would require enforceable, robust data security practices and meaningful notice to consumers. It would also give additional protections to consumers after a breach. Of course, breaches will continue to occur, but they occur more often when there is no accountability and no preventive measures are in place. And our bill will not stop mistakes and cyber crimes from happening, but we need to start somewhere.

So Mr. Smith, I read your op-ed in USA Today last month and the new CEO's op-ed in the Wall Street Journal last week and I appreciate that you are both sorry, but my question is what now? I would like to yield now the remainder of my time to my colleague from New Mexico.

Mr. LUJÁN. Thank you to our ranking member, Mr. Pallone, and I thank the committee's leadership for organizing this important hearing. 145,500 thousand million Americans, 145.5 million people at risk because of Equifax's failure. Now Mr. Smith, the American people deserve answers and I hope you are prepared to provide them. Not just about what caused the breach, but what Equifax is doing to prevent this from happening again and to ensure that those who were harmed are made whole.

I worry that your job today is about damage control, to put a happy face on your firm's disgraceful actions and then depart with a golden parachute. Unfortunately, if fraudsters destroy my constituents' savings and financial futures there is no golden parachute awaiting them. We have questions and it is our expectation that you have concrete answers.

And I hope this hearing is just the start of our committee's work. We need to work together to hammer out real solutions. I recently took a step in that direction by introducing the Free Credit Freeze Act to allow consumers to protect themselves by freezing and unfreezing their credit at no charge. It is unconscionable that Equifax failed so spectacularly to protect people's most sensitive personal data. It is even more reprehensible that the same company profits from the pain that they have caused.

And I certainly hope that we can get some assurances from the committee's leadership that we will have a markup and a hearing on legislation to address this mess, and I hope that assurance can be given before the holidays of 2017. I yield back the balance of my time.

Mr. LATTA. Thank you very much. The gentleman yields back and this concludes our member opening statements. The chair would remind members that pursuant to the committee rules, all members' opening statements will be made part of the record.

Today we have Mr. Richard Smith, the former chairman and CEO of Equifax, Inc., who is here to testify before the subcommittee. Mr. Smith will have the opportunity to give an opening statement followed by a round of questions from our members. And Mr. Smith, you are recognized for 5 minutes. Thank you.

**STATEMENT OF RICHARD SMITH, FORMER CHAIRMAN AND  
CEO OF EQUIFAX, INC.**

Mr. SMITH. Thank you. Chairman Walden, Ranking Member Pallone, Chairman Latta, Ranking Member Schakowsky, and the honorable members of the subcommittee, it is an honor to be here before you today.

My name is Rick Smith and for the last 12 years I have had the honor of being the CEO and chairman of Equifax. Earlier this week, I submitted a written testimony which at this time I don't plan on going through any detail on that but rather I am here today to explain to you and the American people how criminal hackers were able to steal personal information on over 145 million Americans from our servers, and as importantly, to discuss with you today what our company's response was to that criminal hack.

The criminal hack happened on my watch and as CEO I am ultimately responsible and I take full responsibility. I am here today to say to each and every person affected by this breach I am truly and deeply sorry for what happened. I have talked to many consumers, I have read your letters, and Equifax is committed to making it whole for you. Americans have a right to know how this happened and I am prepared to testify today about what I have learned and what I did about this incident in my role as CEO and as chairman of the board, and also what I know about the incident as a result of being briefed by the company's investigation which is ongoing.

We know now that this criminal attack was made possible because of a combination of human error and technological error. The human error involved the failure to apply a software patch to our dispute portal in March of 2017. The technological error involved a scanner which failed to detect that vulnerability on that particular portal. Both errors have since been addressed.

On July 29th and July 30th, suspicious activity was detected and a team followed our security incident protocol. The team immediately shut down the portal and began our internal security investigation. On August 2nd, we hired top cybersecurity forensic and legal experts and at that time we notified the FBI. At that time, to be clear, 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 breach.

Over the weeks leading up to September 7th, our team continued working around the clock to prepare. We took four steps to protect consumers. Step number one, 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. Step two, helping consumers by developing a web site, staffing up massive call centers, and offering services free to every American. Three, preparing for increased cyber attacks which we were advised by the cybersecurity experts that we should expect. And finally, continue to coordinate with the FBI and their criminal investigation of the hackers and also to notify other federal and state agencies.

In the rollout of our remediation program mistakes were made, for which again I deeply apologize. I regret the frustration that many Americans felt when our web sites and call centers were overwhelmed in the early days. It is no excuse, but it certainly did not help that Hurricane Irma took down two of our larger call centers in the first few days after the breach. Since then, however, the company has dramatically increased its capacity and I can report to you today that we have handled over 420 million consumer visits to our web site in just over 3 weeks and the wait times at the call centers have been substantially reduced.

At my direction, the company offered a broad package of services to all Americans. In addition, we developed a new service available on January 31st, 2018 that will give all consumers the power to control access to their credit data by allowing them to lock and unlock their credit files when they want and they can do that for free for life.

Putting the power to control access to credit data in the hands of the American consumer is a step forward. I look forward to discussing this new tool with you during my testimony. As we have all painfully learned, data security is a national security problem. Putting the consumer in control of their credit data is a first step towards a long-term solution to the industry and the problem of identity theft.

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

Chairman Walden, Ranking Member Pallone, Chairman Latta, Ranking Member Schakowsky, and the honorable members of the subcommittee, thank you again for inviting me here today to speak to you. I will close by saying again how sorry I am for this breach. On a personal note, I want to thank the many hardworking and dedicated employees who have worked with me so tirelessly over the past 12 years at Equifax. Equifax is a very good company with thousands of great people waking up every day trying to do what is right. I know they will continue to work tirelessly as we have over the past 2 months to right the wrong. I am looking forward to answering your questions. Thank you.

[The prepared statement of Mr. Smith follows:]

**Prepared Testimony of Richard F. Smith  
before the U.S. House Committee on Energy and Commerce  
Subcommittee on Digital Commerce and Consumer Protection**

**October 3, 2017**

Chairman Latta, Ranking Member Schakowsky, and Honorable Members of the Subcommittee, 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](http://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 Subcommittee 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 Latta, Ranking Member Schakowsky, and Honorable Members of the Subcommittee, 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.

Mr. LATTA. Thank you very much. This concludes our witness testimony and we will move into the question and answer portion of our hearing. I will begin with the questioning and recognize myself for 5 minutes. And I would remind members because we do have quite a few members who want to ask questions today, I am going to try to keep the 5-minute rule on questions in place so you will hear the tapping. But I will begin with the questioning.

Mr. Smith, the timeline of events is raising some red flags I would like to ask you about. According to your statement, the first time you heard about the breach of security was on July the 31st of 2017. Is that correct?

Mr. SMITH. Yes, Congressman. That is correct.

Mr. LATTA. And you first asked for a briefing about the breach on August the 15th. Is that correct?

Mr. SMITH. Yes. That is correct.

Mr. LATTA. And the first time the board of directors was notified about the breach was August the 24th. Is that correct, the full board?

Mr. SMITH. Congressman, on the 22nd of August I notified our lead director, presiding director at the time. The full board was briefed on the 24th and again on the 25th and subsequent meetings after that.

Mr. LATTA. All right. And you notified the public about the breach on September the 7th, correct?

Mr. SMITH. That is correct.

Mr. LATTA. OK. You state in your testimony that you began developing the remediation for consumers on August the 24th or the 25th. Why was there a 10-day delay between you finding out that personal information had likely been stolen and beginning to develop the remediation plan and do you think that 10-day window was responsible for having learned about that personal information being stolen to start talking about how to talk to the consumers?

Mr. SMITH. Congressman, I understand the question, if I may go back to the timeframe of the 31st. So if you go to the 29th and 30th, someone in security had detected what they deemed as suspicious activity. That is something that happens routinely around our business. On the 30th they bring down this particular portal and they start their own internal investigation.

As I had mentioned in my opening comments and in my written testimony, on the 2nd of August they had engaged leading forensic experts, cyber experts, and King & Spalding, a leading law firm, and their cybersecurity team. When you talk to the forensics experts they will tell you the complications of trying to understand where these criminals were, the footprints they had left, the inquiries they had made, is a cumbersome, cumbersome process. That is why it took weeks before we had an indication for the breadth and the depth of the issue which brought us to the August 24th date that you had mentioned.

Mr. LATTA. Well, let me just back up to July the 31st when you learned, again you were talking with the experts at that time and you learned about the breach and you testified that you did not know that personal information had been stolen at that point. But did you ask anyone if personal information had been stolen when you found out about that breach?



Mr. SMITH. Congressman, on the 31st, all I was told at that time was that security had noticed a suspicious movement of data out of an environment we call a dispute portal. It wasn't until later that they understood that was an actual dispute document. We had no indication on the 31st of July there was any PII information that was vulnerable.

Mr. LATTA. OK, so I guess again, but again not knowing if that personal information had been stolen at that time, your company is built on data and at any point did you think it was important if somebody in the company started looking at if personal data had been stolen at that point?

Mr. SMITH. Congressman, I can tell you we are working with the best forensic auditors in the business. They do this for a living. We had a great cyber team from King & Spalding with us. It took them time. At that time they did not know if data had been compromised, exfiltrated, or what the data was.

Mr. LATTA. If we could go back to when you did find out about the breach and that conversation with your chief information officer, Mr. Webb, how did he exactly tell you that there had been a breach? Was it a phone call, an email, in person, or how did he notify you of the breach?

Mr. SMITH. It was a face-to-face brief meeting on the 31st. At that time he had just learned as well, so the data was very fresh to him. The incident was described as an incident not as a breach.

Mr. LATTA. Is that the normal way for that information if there had been a breach at the company to notify someone is for the CIO to come and just give a face-to-face, or is that the standard operating procedure then?

Mr. SMITH. Congressman, at that time we had no indication it was a breach. It was a suspicious activity.

Mr. LATTA. Did you tell anyone else in senior management or any other members of the board of directors about the breach at that time, or is it just not until on August the 22nd when you had the one call and then the 24th for the rest of the board of directors did anyone else know about the breach?

Mr. SMITH. Again, it is important to say on July 31st we did not know it was a breach at that time, suspicious activity only. The first notification to the board was the lead director on the 22nd of August, which followed in the chronology of events a meeting I had with our cybersecurity experts and our outside counsel had occurred on the 17th of August. That is when the picture was starting to develop.

Mr. LATTA. Thank you. My time is expired and I will recognize the gentlelady from Illinois, the ranking member, for 5 minutes.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. I am going to get right to it. I wanted to ask some questions about John Kelley, the chief legal officer, who I understand is responsible for security at Equifax or was at least at the time of the breach and its discovery. Is that right?

Mr. SMITH. That is correct, Congresswoman.

Ms. SCHAKOWSKY. And Mr. Kelley in turn reports directly to you the CEO, correct?

Mr. SMITH. Correct.

Ms. SCHAKOWSKY. OK. So we were told that Mr. Kelley was informed by the chief security officer the week of July 30th—we have just been talking about that—that a cybersecurity incident you mentioned that had occurred. Is that correct?

Mr. SMITH. He was notified, it is my understanding, on the 31st of July.

Ms. SCHAKOWSKY. Thirty first, OK.

Mr. SMITH. That there was suspicious activity in a particular environment called a web portal that was a dispute environment.

Ms. SCHAKOWSKY. We were told that Mr. Kelley—this is our staff—was informed at the same time that the incident might have compromised personally identifiable information. Is that correct?

Mr. SMITH. The only knowledge I have is he was notified on the 31st that there was suspicious activity in a consumer dispute portal.

Ms. SCHAKOWSKY. Well, we were told that Mr. Kelley then wrote a short memo to you regarding the incident. Is that correct?

Mr. SMITH. Correct, Congresswoman. And in his email it said some suspicious activity.

Ms. SCHAKOWSKY. OK. Around that same time, three Equifax executives sold over \$1 million of Equifax stock. That is on August 1st and August 2nd, and it is reported that Mr. Kelley was ultimately responsible for approving those sales. Is it true that Mr. Kelley or one of his direct reports would have been required to sign off on these stock sales?

Mr. SMITH. Yes. Mr. Kelley who is our general counsel owns the clearance process and he would—

Ms. SCHAKOWSKY. I have a lot of questions. So the answer is yes, he was supposed to sign off?

Mr. SMITH. Yes.

Ms. SCHAKOWSKY. Did any one of these three executives have knowledge the cybersecurity incident had occurred?

Mr. SMITH. To the best of my knowledge, Congresswoman, no.

Ms. SCHAKOWSKY. When were they informed that the incident had occurred?

Mr. SMITH. I don't know exactly the date that they were informed, but to the best of my knowledge they had no knowledge at the time they cleared their trades with the general counsel.

Ms. SCHAKOWSKY. Do you know for sure that they didn't know?

Mr. SMITH. To the best of my knowledge they did not know.

Ms. SCHAKOWSKY. And Mr. Kelley, who we were told knew of the breach and that it contained personal information and yet still approved the stock sale, is he still chief legal officer for Equifax?

Mr. SMITH. Congresswoman, I would come back to it again, he did not know it was a breach when he approved—

Ms. SCHAKOWSKY. That it could have been a breach.

Mr. SMITH. All he knew at the time, it is my understanding, is suspicious activity when he approved the sales.

Ms. SCHAKOWSKY. What the heck does suspicious—it could be a breach, right?

Mr. SMITH. It was deemed suspicious activity. We had no indication that PII was in fact compromised at that time. We had no idea if data was exfiltrated at that time.

Ms. SCHAKOWSKY. So now I understand that you agreed to forego your 2017 bonus which has been about \$3 million for the past 2 years, correct?

Mr. SMITH. That is correct.

Ms. SCHAKOWSKY. But it has been reported that you will still retain \$18 million in pension benefits from Equifax; is that accurate?

Mr. SMITH. That is correct.

Ms. SCHAKOWSKY. Retiring, which is the category right now although the company maintains the right to change that designation, also means you will be free to sell your Equifax stock which is worth about \$24 million. Is that correct?

Mr. SMITH. Congresswoman, that calculation, it is hard to say. It is a complicated calculation. It depends on the total shareholder return of the company at the time the stocks vest. There are multiple variables. That may be an estimate, I have seen different estimates, but it is hard to say what that number is and we won't know until the end of the year.

Ms. SCHAKOWSKY. And that is in addition to Equifax stock you sold earlier in this year for \$19 million. Is that correct?

Mr. SMITH. That sounds correct.

Ms. SCHAKOWSKY. And according to one report, you could be eligible for \$22 million in performance-based compensation depending how Equifax stock performs in the next 3 years. Is that right?

Mr. SMITH. Let me be very clear, if I may, Congresswoman. When I announced my retirement and thought it was best for the company to move forward with a new leader, I agreed to step down at that time with no further compensation. I agreed I should not get a bonus. I agreed there would be no severance. I asked for nothing beyond what I had already earned.

Ms. SCHAKOWSKY. I was just informed by staff that the chief security officer told the chief legal officer verbally that there was PII that according to a call with staff yesterday that actually there was a mention of the breach of personally identifiable information. The CSO told us in a call yesterday is what I just heard from staff.

Mr. SMITH. Congresswoman, I have no documentation, no insight, no knowledge that anyone in the company had informed me or in that case the chief general counsel that there was a breach on July 31st. Is that what you said?

Ms. SCHAKOWSKY. Yes. No, we didn't say a date. I am told that our staff didn't say a date. OK, let me just say I am glad the FBI is looking into it and many state attorneys general. The City of Chicago has sued, so we will probably get more information that way as well. Thank you.

Mr. LATTA. Thank you very much. The gentlelady's time has expired. The chair now recognizes the chairman of the full committee, the gentleman from Oregon, for 5 minutes.

Mr. WALDEN. Thank you, Mr. Chairman.

Mr. Smith, thanks again for being here today. As you know, this is an example of an Equifax credit report in my hand. It lists social security numbers, addresses, credit history, debts, all the sort of personal financial information. It is the lifeblood of Equifax, right? These data points are really, really important to what you do as a company?

Mr. SMITH. Congressman, that is correct.

Mr. WALDEN. It is a \$3 billion company, data on 820 million customers worldwide, and yet it appears this breach happened because the company didn't know it was running certain software on its system, right, the Apache Struts software that had the patch requirement?

Mr. SMITH. Congressman, as I alluded to in my opening comments and the written testimony, there was a human error and a technology error that did not allow us to identify and cover.

Mr. WALDEN. And I think that is what we are trying to get to here. If I understand it right, your own information technology system did not tell the Equifax security division that the Apache Struts software, which contained the vulnerability that led to this breach, was running on the Equifax system. How did that happen?

Mr. SMITH. Congressman, the day after the notification came out from CERT, the security team notified a wide range of people in the technology team who were responsible for then finding the vulnerability, applying the patch, and then, days later as is typical protocol, to deploy a technology scanner to go then look for the vulnerability, find the vulnerability, and if it found a vulnerability it knew it was not patched. Both human deployment of the patch and the scanning deployment did not work. The protocol was followed.

Mr. WALDEN. OK, so then people ask us how does that happen? If as sophisticated of a company as you headed is with so much at risk, how does this happen? And, we have colleagues that say we are going to double the fines, triple the fines, put fines in, do all these things, but how does this happen when so much is at stake? I don't think we can pass a law that, excuse me for saying this but I can't fix stupid, as a colleague of mine used to say. With so much at risk—I have talked to other software companies and people in this space who say some companies have an automated system that when a patch comes out it automatically gets installed. That is not what you had necessarily, right?

Mr. SMITH. I am unaware of an automatic patch. The system we have in place is security gets notification and it is not uncommon to get notification from software providers routinely about vulnerabilities that are discovered.

Mr. WALDEN. Right.

Mr. SMITH. They follow the protocol, which is to notify the appropriate people within the timeframe that the protocol called for. Unfortunately, the human error was they did not find the patch. Did not know—

Mr. WALDEN. If I could, the human error piece you reference is that they didn't know that that particular software was running on your system, Apache Struts was running? Because that is what needed patching, right?

Mr. SMITH. Congressman, great question, if I may clarify.

Mr. WALDEN. Yes, please.

Mr. SMITH. The human error was the individual who is responsible for communicating in the organization to apply the patch did not.

Mr. WALDEN. So does that mean that that individual knew that the software was there and it needed to be patched and did not communicate that to the team that does the patching? Is that the heart of the issue here?

Mr. SMITH. That is my understanding, sir.

Mr. WALDEN. I was on a bank board for a while and we always had double checks on everybody, right. Do you not have a double check of some sort, an audit of some sort? It seems like that was a single point.

Mr. SMITH. The double check was the scanning device that was deployed a few days later.

Mr. WALDEN. But did the scanning device—I don't know how that process works. Does it know you have that software or do you have to tell it that is what you are scanning for?

Mr. SMITH. It is the latter. You have got to tell it what it is looking for. It scans the environment looking for—

Mr. WALDEN. And so the individual who didn't tell the IT team, that is where the individual failed. Was that the same person telling them what to look for?

Mr. SMITH. No. The scanner is deployed by the security team. And I should clarify there that the rationale or the reason why the scanner or the technology piece did not locate the vulnerability is still under investigation by outside counsel.

Mr. WALDEN. All right, one final question. You have referenced the suspicious movements of data. You have referenced incident. The American people think all of that is breach. How regularly did you have incidents or suspicious movement of data? Is this a routine thing that people call, hey, we had another incident, we have another suspicious movement of data, or was this outside normal operations?

Mr. SMITH. Congressman, thank you for that question. As you alluded to in your comments, we do have a lot of data and our primary goal is to protect that data. And we have experienced millions of suspicious activities against our database any given year.

Mr. WALDEN. But to the point that the head of your security team comes to you and says, hey, we have another one?

Mr. SMITH. Oh. That is not uncommon. It is not uncommon.

Mr. WALDEN. How often would that happen in the course of a week that they would come to the CEO and say heads up?

Mr. SMITH. I don't have a number for you, Congressman, but it is not uncommon. It is not uncommon for us to engage forensic audit firms. It is not uncommon for us to engage outside counsel to help us think things through when there is suspicious activity. It is a part of doing business in a data business as you alluded to.

Mr. WALDEN. Thank you for the indulgence of the committee. I yield the balance of my time.

Mr. LATTA. The gentleman yields back and the chair recognizes the ranking member of the full committee, the gentleman from New Jersey, for 5 minutes.

Mr. PALLONE. Thank you.

Mr. Smith, you testified that on August 11th you were informed that hackers had stolen, "a large amount of consumers' personally identifiable information," in this incident. And on August 17th, I guess a week later, you said in a speech, "fraud is a huge opportunity for Equifax. It is a massive, growing business for us." So I am just looking for a number, Mr. Smith. At the time you gave that speech, roughly how many consumers did you believe had been compromised by the breach, if you could?

Mr. SMITH. Congressman, if I may clarify, I think you alluded to an August 11th date?

Mr. PALLONE. August 11th, initially, and then August 17th in the second speech.

Mr. SMITH. August 11th I had no indication. I was not informed at that time. My notification was before the August 17th meeting. And you alluded to a speech?

Mr. PALLONE. Well, yes. On the 17th you said in a speech, fraud is a huge opportunity for Equifax. It is a massive growing business for us. I am just looking for a number. At the time, roughly, how many consumers did you believe had been compromised by the breach?

Mr. SMITH. On August 17th, which is I think on or around the date you had talked about that I gave a speech, we did not know how much data was compromised, what data was compromised. That story was still developing. And that speech you are alluding to is a very common speech we have in communities. I think this happened to be at a university that we talked to them, but at that time when I gave that speech I did not know size, the scope of the breach.

Mr. PALLONE. All right. During your tenure at Equifax you expanded the company's business into packaging and selling other people's data. And in that August 17th speech you explained that having free data with a gross margin of profit of about 90 percent is, "a pretty unique model." And I get that this unique model is a good deal for Equifax, but can you explain how it is a good deal for consumers?

Mr. SMITH. Thank you, Congressman. I think I understand the question. Our industry has been around for a number of years as you know. In fact, Equifax is a 118-year-old company. We are part of a federally regulated ecosystem that enables consumers to get access to credit when they want access to credit and hopefully at the best rates available to them at that time. So we are very vital to the flow of the economy not just in the U.S. but around the world.

Mr. PALLONE. All right. And I want to turn to what Equifax is offering consumers in the wake of this breach, specifically the free credit lock service that is supposed to be introduced next year. We have been told that this free credit lock service could require consumers to consent to Equifax sharing or selling the information it collects from the service to third parties with whom the individual already has a business relationship for marketing or other purposes. Is that true?

Mr. SMITH. This product will be a web-enabled, mobile-enabled application that will allow a consumer at the time he or she, if they decide they want access to credit, can simply toggle on and toggle off that application to give the bank, credit card issuer, auto lender, access to their credit file to approve their own.

Mr. PALLONE. Well, by agreeing to use the Equifax's lock service will consumers also be opting in to any additional marketing arrangements either via Equifax or any of its partners?

Mr. SMITH. Congressman, we are trying to change the paradigm, and what I mean by that is this will be in an environment viewed as a service, a utility not a product. But we know cross-selling, up-

selling, or any products available to the consumer, when they go to get and sign up for the lock product it is a service to them and that is the only product the service will be able to get.

Mr. PALLONE. Now will Equifax give consumers an easy and free method to choose not to share their data in this way, even if the consumer already has a business relationship with the third party?

Mr. SMITH. Yes, Congressman. I would envision as this evolves over time the consumer will have the ability to invite into their world who they want to have access and who they do not. It will be their choice, their power, not ours, to make that decision.

Mr. PALLONE. Now last week, the interim CEO announced that by January 31st of 2018 Equifax would make locking and unlocking of a person's Equifax credit report free forever. A credit report lock is already included in TrustedID Premier and other services like credit monitoring and identity theft insurance. Will that still end after 1 year?

Mr. SMITH. Congressman, a couple of differences. Number one, the product we offer today for consumers protects the consumer at the same level of protection they would get January 31st. The difference is today it is a browser-enabled product or service. The 31st of January it will be an application, much simpler and easier for the consumer to use. The protection is largely the same.

So they get this free service when they sign through for 1 year. At the end of the 1 year, effective January 31st of 2018, it goes into the new lock product.

Mr. PALLONE. I guess, the difference other than not expiring between the credit report lock that is part of TrustedID Premier and the credit locking tool that will be available in January, why not just extend the freeze program?

Mr. SMITH. There is a difference between the freeze product which came to pass with FACTA back in 2003, passed into law in 2004. That is now governed by state laws in all states and it is a cumbersome process for a consumer. In many cases, some states require you to mail in your request for a freeze and then we must mail you a PIN, so your ability to get access to get credit when you want credit is encumbered.

A consumer could go to a car dealer or to a bank to get a credit card, forget his or her PIN on a freeze product. Have to go back home, look for the PIN, mail the PIN in. So it is a cumbersome process. The lock product we are offering today is a big step forward. The lock product for the 31st of January is an even further step forward.

Mr. PALLONE. My time has run out, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman's time has expired. The chair now recognizes the chairman emeritus of the full committee, the gentleman from Texas, for 5 minutes.

Mr. BARTON. Thank you, Mr. Chairman, and since I am not a member of this subcommittee, thank you for your courtesy in allowing me to ask questions.

Mr. Smith, what is the market value of Equifax? What is your company worth, or your former company?

Mr. SMITH. Congressman, last time I checked it is somewhere close to \$13 billion.

Mr. BARTON. Thirteen billion. I am told by my staff that this latest data breach was about 143 million people; is that right?

Mr. SMITH. We were informed yesterday from the company that it is typical in a forensic audit there was some slight movement and the numbers-adjusted press release came out from the company last night it is 145.5.

Mr. BARTON. Well, OK. I appreciate your accuracy there. But under current law you are basically required to alert each of those that their account has been hacked, but there is really no penalty unless there is some sort of a lawsuit filed and the Federal Trade Commission or a state attorney general files a class action lawsuit against your company. So you are just required to notify everybody and say so sorry, so sad. I understand that your company has to stay in business, has to make money, but it would seem to me that you might pay a little bit more attention to security if you had to pay everybody whose account got hacked a couple of thousand bucks or something. What would the industry reaction be to that if we passed a law that did that?

Mr. SMITH. Congressman, I understand your question. I think the path that we were on when I was there and the company has continued is the right path, and that is the path of allowing the consumers to control the power of who and when accesses their credit file going forward, taking the——

Mr. BARTON. Well, the consumer can't control the security of your system.

Mr. SMITH. That is true, sir. But they can control——

Mr. BARTON. And your security people knew there was a problem and according to staff briefings that I have been a part of they didn't act in a very expeditious fashion until the system had already been hacked. You are to be commended for being here. I don't think we subpoenaed you. I think you appeared voluntarily, which shows a commendable amount of integrity on your part.

But I am tired of almost every month there is another security breach and it is OK, we have to alert you. I checked my file to see if I was one of the ones that got breached, and apparently I wasn't. I don't know how I escaped, but I didn't get breached. But my staff person did, and we looked at her reports last night and the amount of information that is collected is way beyond what you need to determine if she is creditworthy for a consumer loan. Basically, her entire adult history going back 10 years everywhere she has lived, her name, her date of birth, her social security number, her phone numbers, her addresses, her credit card, student loans, security clearance applications for federal employment, car insurance, even employment history of jobs that she worked when she was in high school. That is not needed to determine whether she is worthy of getting a \$5,000 credit card loan or something and now it is all out in the netherworld of whoever hacked it.

I can't speak for anybody but myself, but I think it is time at the federal level to put some teeth into this and some sort of a per-account payment. And again I don't want to drive credit bureaus out of business and all of that, but we could have this hearing every year from now on if we don't do something to change the current system.



So I would hope that you would go back to your peers and work with the committee, the chairman and the subcommittee chairman and ranking member and let's figure out something to do that actually gives an incentive to the industry to protect ourselves. And the only way I know to do it is some fine per account hacked that is large enough that even a company that is worth \$13 billion would rather protect their data and probably not collect as much data than just come up here and have to appear and say we are sorry.

With that, Mr. Chairman, thank you for your courtesy and I yield back.

Mr. LATTA. The gentleman yields back and the chair now recognizes the gentleman from New Mexico for 5 minutes.

Mr. LUJÁN. Thank you, Mr. Chairman.

Mr. Smith, there is a difference between a lock product and a freeze, correct; those are two different things?

Mr. SMITH. Congressman, there is a process. It is a little different, but as far as the consumer and the protection that he or she would get from doing one versus the other is virtually if not exactly the same.

Mr. LUJÁN. Well, virtually almost exactly is not the same. Are they different?

Mr. SMITH. It is the same.

Mr. LUJÁN. So your lock product is the same as a freeze?

Mr. SMITH. As far as the protection—

Mr. LUJÁN. Well, we will get into that later. I appreciate that clarification. Will Equifax be willing to pay for this freeze at Experian and TransUnion for consumers whose information was stolen?

Mr. SMITH. You are referring to the freeze or the lock?

Mr. LUJÁN. You said they are the same so.

Mr. SMITH. Yes. Right now we offer a free lock product as you know for 1 year and then a free lifetime lock product for life starting January 31st, 2018.

Mr. LUJÁN. And that also extends to Experian and TransUnion?

Mr. SMITH. No, sir. It does not.

Mr. LUJÁN. Let me repeat the question. Will Equifax be willing to pay for that freeze for that lock at Experian and TransUnion for consumers whose information was stolen through Equifax?

Mr. SMITH. Congressman, the company has come out with what they feel is a comprehensive five different services today and a lifetime lock. I would encourage TransUnion and Experian to do the same. It is time we changed the paradigm, give the power back to the consumer to control who accesses his or her credit data. It is the right thing to do.

Mr. LUJÁN. OK. I am down to limited time, Mr. Smith. I apologize. I will take that as a no that Equifax will not pay for Experian and TransUnion consumers. Do you think consumers should have to pay a penalty for your mistake including potential identity theft, false credit accounts, fraudulent tax returns, or medical identity theft, or do you commit to compensating any consumers who suffer harm as a consequence of your breach?

Mr. SMITH. We take this seriously. I have apologized. I will apologize again to the American consumer. We have offered a comprehensive set of products for free.

Mr. LUJÁN. Mr. Smith, will those comprehensive sets of products make consumers whole?

Mr. SMITH. It will protect them going forward.

Mr. LUJÁN. Will it make them whole, yes or no?

Mr. SMITH. It is hard for me to tell if someone has been harmed so I can't answer the question.

Mr. LUJÁN. If someone's credit has been stolen and someone went and opened up a bunch of their accounts, bought furniture, bought cell phones, bought a bunch of fuel, and now this consumer can't fix their history they have been harmed. In that case will Equifax make that person whole?

Mr. SMITH. Congressman, as I have said I apologize. We have offered them a—

Mr. LUJÁN. Thank you very much, sir.

So I want to go back to the line of questioning earlier from Mr. Pallone. On August 11th, in your prepared testimony it says that you were aware of a large amount of consumer PII. On August 15th, it says in your prepared testimony a PII had been stolen, it appeared likely, and that you requested a detailed briefing to determine how much the company should proceed. On August 17th, it says, you, I held a senior leadership meeting to receive the detailed briefing on the investigation. You gave a speech also on the 17th about profiting off of fraud with these new markets. You shared with Mr. Pallone that you were not aware of PII being stolen. What is it?

Mr. SMITH. Congressman, on the 17th I had the full debrief from Mandiant, our forensic auditors, from outside counsel, and my team. I was aware on the 15th that there had been some PII compromise. How much the scope—

Mr. LUJÁN. I appreciate that clarification. You were aware it was stolen and you just were not aware how much?

Mr. SMITH. I was not aware it was stolen. I was aware there was—

Mr. LUJÁN. It says in your prepared testimony that you were aware, that you asked for a detailed briefing to determine how the company should proceed. So you were aware that PII was stolen on the 15th; is that true or not true?

Mr. SMITH. At that time, the 17th was the detailed review of when I learned about PII. And even at that time which PII, was it stolen, was it not stolen, those details came to life, Congressman, over the course of August.

Mr. LUJÁN. Mr. Smith, on August 15th, were you aware that there was PII that was stolen or not?

Mr. SMITH. On August 15th—

Mr. LUJÁN. Regardless of the amount were you aware of that?

Mr. SMITH. On August 15th, I was made aware that hackers, criminal hackers, had gotten into our system and had some PII information.

Mr. LUJÁN. OK. Well, we can revert to your prepared testimony. The other question that I have that Ms. Schakowsky was asking on, is Chief Legal Officer John Kelley still employed by you, or by Equifax?

Mr. SMITH. Yes, he is.

Mr. LUJÁN. And you were the CEO at the time that approved the terms of the retirement for David Webb and Susan Mauldin. Is their classification as retired permanent or could it potentially change to fired for cause like yours?

Mr. SMITH. There is an investigation going on by the board at this time.

Mr. LUJÁN. And Mr. Chairman, I know that my time has collapsed here, if you will, but there is an article in WGN-TV that talks about Equifax doing their own investigation into the three executives that sold their stock and profited. And I guess they must have a pretty good investigative team there because between the press release that happened on Friday or whenever it came out, and then a story on Sunday, and today we have a revelation that those folks didn't know that this breach took place, I just hope we get to the bottom of this.

And again, Mr. Chairman, I hope that we can be given assurance to the committee and to the American people that this committee will have a markup and a hearing with bills that we can take to the floor before the holidays to give the American people consumers confidence again because this is a mess. Thank you, Mr. Chairman.

Mr. LATTI. Thank you very much. The gentleman's time has expired. And the chair now recognizes the gentleman from Mississippi, the vice chairman of the subcommittee, for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman.

Mr. Smith, thank you for being here to testify today. In your written testimony and in response to some of the chairman's questions, you stated that you were informed of suspicious activity on July the 31st by your chief information officer and went on to discuss that. And you said, I certainly did not know that personal identifying information, PII, had been stolen or have any indication of the scope of the attack. Did you ask him if there had been any personal identifying information that had been obtained?

Mr. SMITH. Congressman, at that time I was informed it was a dispute portal document. A dispute portal document is something that typically houses if the company is disputing with us they paid off a utility bill he or she may take a picture of the utility bill. So at that time that was the conversation.

Mr. HARPER. Mr. Smith, not to interrupt, but my question was did you ask if any PII had been accessed?

Mr. SMITH. No, I did not.

Mr. HARPER. Were you made aware at that point of the Apache Struts patch?

Mr. SMITH. No, sir. I was not.

Mr. HARPER. Had you had any meetings with your chief information officer or your security department about any of this issue prior to July 31st?

Mr. SMITH. No, Congressman. I did not.

Mr. HARPER. Had you had any meetings with them about any other security information during that time from March until July 31st?

Mr. SMITH. Oh yes. We would have routine meetings, security reviews, IT reviews.

Mr. HARPER. How often do you have those?

Mr. SMITH. Common due process would be at least quarterly.

Mr. HARPER. And why did you not have this discussion come up and did you have, obviously that is more than a quarter, so how many meetings did you have between that time of March the 8th until July the 31st with your security team?

Mr. SMITH. Make sure I understand your question. Why didn't—

Mr. HARPER. No. How many meetings did you have during that time from March the 8th until July the 31st?

Mr. SMITH. I don't have that information with me. If that is important we can get that.

Mr. HARPER. Well, how many do you remember? Do you remember any of those?

Mr. SMITH. So normally we would have IT reviews at least quarterly and security reviews at least quarterly. And then you would augment that on an as-needed basis.

Mr. HARPER. Well, with those meetings and those timelines of March the 8th until July 31st we are covering into three quarters. Not a total of 9 months, but you touch into three quarters of that year. And at any point in any of that did you have any information about this going on?

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

Mr. HARPER. All right. In your testimony you indicate that the security department ran scans in March for the vulnerability but failed to identify it. Can you explain how this is possible and why was there never any confirmation of anybody coming back and checking to see, OK, we have this identified information, there was a failure of someone on the team to identify this that it was being used, that the software was even being used? Was there no one coming in to verify that? Do you have any outside person prior to the ones that you hired to look at this?

Mr. SMITH. Congressman, we get notifications routinely, the IT team and security team do, to apply applications. This individual as I mentioned earlier did not communicate to the right level to apply the patch. The follow-up was as you mentioned—

Mr. HARPER. You said this individual?

Mr. SMITH. Yes.

Mr. HARPER. So you had one person responsible for this?

Mr. SMITH. There is an owner of the patch process. There is a communication that comes out from security. It is a broad-based communication. Once they receive notification from a software company, or in this case DHS, they notify appropriate people. Then an individual who owns the patch process cascades that communication.

Mr. HARPER. For everyone who is on your Equifax team is there anything more important than protecting the PII of the consumers?

Mr. SMITH. No, sir.

Mr. HARPER. Would you identify that as the number one responsibility of the company and everybody in your company?

Mr. SMITH. We have for years, sir, yes.

Mr. HARPER. OK. So it just appears, obviously, the job wasn't done and so we know that and we are trying to look at this. And I know too there was an Equifax spokeswoman who said, we have taken short-term mediation steps and continue to implement and

accelerate long-term security improvements as part of ongoing actions to help prevent this type of incident from happening again.

So we have 145.5 million people whose PII has been compromised. How many files do you have in the system?

Mr. SMITH. Worldwide?

Mr. HARPER. Yes, sir.

Mr. SMITH. I think someone mentioned earlier there is a public number out there of over 800 and some odd million consumers and 100 million companies, roughly.

Mr. HARPER. And we know this breach includes some from Canada, some from the U.K. Would that be fair to say even at this point?

Mr. SMITH. Congressman, a point of clarification there, there was some data that we had on, I think it is 7,000 Canadians in the U.S. So the data was in the U.S., same environment. We had some data on U.K. citizens also in the U.S. That piece is still under investigation.

Mr. HARPER. My home State of Mississippi has three million people. Almost 1.4 million files have been breached in my state. If you take away people that are minors who don't have a file yet, almost my entire state is going to be impacted. So this is a travesty, something that was preventable, we know, and so saying that we want to protect what goes forward doesn't bring us a lot of comfort today. Thank you and I yield back.

Mr. LATTA. The gentleman yields back. The chair now recognizes the gentleman from California for 5 minutes.

Mr. CÁRDENAS. Thank you very much. I thought I prepared for this committee, but I have more chicken scratch notes. I don't even know where to start.

Mr. SMITH, welcome to Washington. Are you currently employed by Equifax?

Mr. SMITH. No, sir.

Mr. CÁRDENAS. You are not. When you decided to come before this committee were you specifically requested by name to come to this committee by this committee or were you offered up by Equifax as the representative of Equifax to come represent Equifax before this committee?

Mr. SMITH. I believe I was asked specifically to come before the committee.

Mr. CÁRDENAS. By Equifax or the committee?

Mr. SMITH. My understanding is by the committee.

Mr. CÁRDENAS. OK. OK. Apparently the committee asked for the CEO at the time and at that time you were still the CEO, but you are no longer the CEO. Did you inquire as to why the current CEO or interim CEO didn't come before this committee?

Mr. SMITH. I did not, but I felt personally it was my obligation. The breach occurred under my watch. And as I said in my written testimony and my oral testimony I ultimately take that responsibility, so I thought it was important that I be here.

Mr. CÁRDENAS. Thank you. I get the picture. On August 31st or, excuse me, on July 31st you were notified of the suspicious activity that eventually as we now know was a 145 million person breach? Was it July 31st, was it?

Mr. SMITH. Yes, Congressman. It was a brief interaction—

Mr. CÁRDENAS. A verbal interaction?

Mr. SMITH. Yes.

Mr. CÁRDENAS. And then you just referenced as an answer to another one of my colleagues' questions on that on August 31st you received some kind of email referring to the possible breach?

Mr. SMITH. A point of clarification, I was notified on the 31st of July by the chief information officer, Dave Webb, in a very brief interaction that this portal seemed to have a suspicious incident. There was a communication trail internally between others that also referenced that I was aware of this incident through my interaction with Dave Webb.

Mr. CÁRDENAS. So that written trail was not directed to you, you were just mentioned in that trail that you had been verbally notified?

Mr. SMITH. That is my recollection.

Mr. CÁRDENAS. OK. Mr. Chairman, is it appropriate for this committee to ask for that trail of documents?

Mr. LATTA. For our counsel, but I would say—

Mr. CÁRDENAS. OK. Well, if it is appropriate, Mr. Chairman, what I would like is for my office and this committee to receive copies of that trail. That it has been referenced more than once to some of our questions here on this committee, on this congressional committee.

It has come to my attention that several people are no longer with the corporation. You are not officially with the corporation anymore. The CIO at that time is no longer the CIO of the corporation, of Equifax?

Mr. SMITH. That is correct.

Mr. CÁRDENAS. And then there is another higher-up that is no longer—

Mr. SMITH. The chief security officer.

Mr. CÁRDENAS. OK, chief security officer. However, John Kelley was the chief legal officer at that time but still is currently the chief legal officer, correct?

Mr. SMITH. That is correct.

Mr. CÁRDENAS. OK. Apparently, the chief legal officer on or about, between July 29th and August 1st went to outside counsel and hired outside counsel. Correct?

Mr. SMITH. No, Congressman. What occurred on August 2nd is that the chief security officer reached out to a forensic expert, cyber expert, and outside counsel King & Spalding, and she engaged them at that time.

Mr. CÁRDENAS. OK, thank you. When executives at Equifax want to sell stock they need to get the chief legal officer to sign off?

Mr. SMITH. Yes, correct, Congressman. There is a protocol that requires the general counsel of Equifax to approve that sale.

Mr. CÁRDENAS. OK. And John Gamble, Joseph Loughran, Rodolfo Ploder, they are all high-ups with Equifax. They apparently sold stock on or about August 1st or 2nd in the amount of approximately 1.8 million, give or take. So they had to get an OK from John Kelley before they did that, correct?

Mr. SMITH. That is correct, sir.

Mr. CÁRDENAS. OK. And apparently they did get the OK?

Mr. SMITH. Yes. That is my understanding.

Mr. CÁRDENAS. And you were the CEO at the time that they sold that stock?

Mr. SMITH. And I have no step in that——

Mr. CÁRDENAS. I get it.

Mr. SMITH. Yes. I was——

Mr. CÁRDENAS. I am referring to John, but you were the CEO at the time.

Thank you, Mr. Chairman. Just a little bit of latitude on my time. Just a little bit, please. What I would like to request of you, Mr. Chairman, and also the Ranking Member Schakowsky, that we ask for a specific hearing of this committee where we get John Kelley, chief legal officer, who was then the chief legal officer of Equifax and who is currently still the chief legal officer, hopefully when and if we get him here he will still have that title.

I am a bit disturbed that we are Congress holding a hearing and that Equifax has before us someone who no longer works for them. Thank you very much, Mr. Chairman. I hope that we can ask for that hearing where we have John Kelley, the chief legal officer, before us.

Mr. LATTA. Thank you very much. The gentleman's time has expired and the chair now recognizes the former chair of the full committee, the gentleman from Michigan, for 5 minutes.

Mr. UPTON. Thank you, Mr. Chairman.

Mr. Smith, every family watches over their financial data with great concern. It impacts their daily life whether it is going to get a mortgage, a loan, a car, they have to have that credit score that gets them often even a job. So they view that data as it relates to them as very, very private and they want it to be secure.

Here is an Equifax credit report for somebody that I know. It is 131 pages long, unbelievable in terms of the data that has been collected on this particular individual. I would guess that most individuals have no clue that there is that much data that has been assembled on their own personal family account.

Now you said earlier that the data was compromised. So a question that I have to ask is does that word "compromise" include the word or the term "manipulated"? Are those folks who broke into that account, are they able to actually change the accurate data that might be reflective of their own personal story? Can that be changed?

Mr. SMITH. Congressman, I understand your question. The database was attacked by criminals, that we know. The forensic experts that we engaged in this case, Mandiant, has led us to believe that there is no indication the data that is left behind has been manipulated.

Mr. UPTON. Now one of the things that is in this report, any credit report, is you verify the income of that individual to make sure that it is accurate. And as I understand it, and I go again in personal experience, when one goes to get a loan whether it is a mortgage or a car, often one of those little boxes that you check is that you are allowing permission to look at that tax return of the individual. Is that not correct?

Regardless of self-employed income, regardless of automated underwriting findings, when self-employed income is used to qualify, the following documentation is required: most recent 2 years of

their individual tax returns with all schedules and W-2s and K-1s; most recent 2 years' business returns; IRS forms 1120 and 1120S; 1065s in which the borrower has ownership interest at 25 percent or more; and a complete and signed IRS form 4506-T is required for every borrower on the loan application. Tax transcripts validated from the IRS are required for each year documented in the loan file.

So the question is if that is collected, is someone who is a bad actor actually able to use the personal information stolen from this report to then perhaps file a false tax return come the first of the year?

Mr. SMITH. Congressman, I think I understand your question. A couple points of clarification. A credit report does not contain employment and income information. There are many lenders who will ask you as a consumer when going to get a loan to validate your income and there are many means as you alluded to in your readings there as to how you might do that. But the credit report does not contain employment income data.

Number two, the unfortunate criminal hack that we referred to this morning in written testimony and press release over the past month or so was clear to say it did not include the credit report information that you just picked up there. It was limited to nonetheless a large number, but limited to an environment we call a consumer dispute portal, not the credit file itself.

Mr. UPTON. The last question I have is how did you know? We have had a lot of hearings, a number of them classified. Breaches made into Department of Energy, utilities, a whole number of different major players where hackers are coming in trying to break and penetrate daily. What tripped these guys up? How did you identify in fact a breach had been made? What was their mistake?

Mr. SMITH. Congressman, there is a piece of technology called a decryptor, and it was a decryptor that allowed us to see some of the data. And once we saw the data that is what the start of the conversation earlier in the testimony here, that is when we saw the suspicious data and were able to shut off the portal at the end of July.

Mr. UPTON. Yield back, my time is expired.

Mr. LATTA. Thank you very much. The gentleman yields back and the chair now recognizes the gentlelady from Michigan for 5 minutes.

Mrs. DINGELL. Thank you, Mr. Chairman.

Mr. Smith, I first want to say we appreciate your coming and testifying today. We have spent a lot of time talking today about the what, the when, the where, and the whys of this breach and I agree with all of my colleagues that we need to be expressing extreme displeasure.

But I want to ask a few questions about where we go from here, because I hope this has awoken the American consciousness about privacy and credit that they need to be paying far more attention to. This breach is different than most. Not only the scale of those affected but the type of information taken. In the past, folks usually just changed your passwords, maybe you got a new credit card and that was it. It was an annoyance but it had no real impact on your life.



That is not so simple when it is your social security number or other personal information. You can't change your social security number and I can't change my mother's maiden name. This data is out there forever. Clearly something needs to be done. We can all sit here and talk about what went wrong, but we are doing the public a disservice to not at least begin the discussion on how to improve data security. That is why I am a proud co-sponsor of Representative Schakowsky and Ranking Member Pallone's bill. It is a good first step that needs to be given serious consideration. And I am also introducing the Data Protection of 2017. Whatever path we choose going forward, it is important that we take action on the topic and that all American consumers pay attention.

Now I would like to ask a few questions. Nobody has asked this question yet, so just a quick yes or no. Have you or anyone on your team seen signs that the attackers were backed by a nation state?

Mr. SMITH. Congresswoman, we have engaged the FBI. At this point that is all I will say.

Mrs. DINGELL. I don't think it is all the same, but thank you. After your security department blocked the suspicious traffic you mentioned in your testimony, did anyone from your team or outside companies venture beyond the parameter of your network to attempt to locate where they came from?

Mr. SMITH. Congresswoman, yes. We have the ability to track the IP address of the criminals, but as you know finding the location where the IP address does not necessarily tell you where they are from. It is easy to set up IP addresses anywhere in the world.

Mrs. DINGELL. I think we all care about this, but I want to move to this other topic. I share your belief that placing control of access to consumers' credit data should be placed in the hands of the consumer, but most people have no idea that Equifax was even holding their data. I unfortunately learned a long time ago because this isn't the first data theft and Doris and I were part of something else where they got our social security numbers and mother's maiden names.

It is one thing to take steps to mitigate damages after a breach has occurred, but going forward we must give consumers the chance to protect themselves before a breach happens. Do you believe that consumers can take reasonable steps to secure their identity and information if they don't even know who has it?

Mr. SMITH. Congresswoman, I think we can help. I think we can help by the announcement of this offering to all Americans the ability to lock and unlock your credit file for life for free. There needs to be a greater awareness, I understand your point clearly. And I think making this available to all Americans is one step in doing that.

Mrs. DINGELL. So I was just actually even educating my colleagues up here about Credit Karma and they were stunned by how easy it was with two little factoids to suddenly unleash the amount of money they had in every one of the credit card companies, what any data inquiries have been, and all of the different factors. I think most people don't understand that it is not just you, but Experian and TransUnion who are also collecting this data.

Why do consumers have to pay you to access their credit report? Why should that data not be free?

Mr. SMITH. Congresswoman, the consumer has the ability to access the credit report for free from each of the three credit reporting agencies once a year, and you combine that with the ability to lock your credit file for life for free again is a step forward.

Mrs. DINGELL. Well, I am running out time. But like my colleague over here, when you find mistakes, which a number of us have and we are luckier than 99 and 9/10ths, it is very difficult to fix and when you do fix it you still have to pay. I think we need a longer debate about who owns this data and how we educate the American people. Thank you, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentlelady's time has expired and the chair now recognizes the gentleman from New Jersey for 5 minutes.

Mr. LANCE. Thank you, Mr. Chairman.

Good morning to you, Mr. Smith. Criminals perpetrated this fraud. Is it possible that these criminals are from another country?

Mr. SMITH. Congressman, it is possible but at this time—

Mr. LANCE. It is possible. Number two, is it possible it is the government of another country?

Mr. SMITH. As I mentioned to the congresswoman a few minutes ago, we have engaged the FBI they will make that conclusion.

Mr. LANCE. Do you have any suspicions in that regard either persons from other countries or the government of another country?

Mr. SMITH. Congressman, I will defer that. We have the FBI involved.

Mr. LANCE. Yes, I know we have the FBI involved. Do you have an opinion to the two questions I have just asked?

Mr. SMITH. I have no opinion.

Mr. LANCE. You have no opinion. The stock that was sold by your colleagues, Mr. Gamble and Mr. Loughran—I hope I am pronouncing that right—Mr. Ploder, as I understand it that stock was sold on August 2nd. Is it usual that executives of a mature company, not a company that has just come onto an Exchange, is it usual that the significant amounts of stock are sold?

Mr. SMITH. Congressman, a few points here of clarification. The stock was sold on the 1st and the 2nd. So—

Mr. LANCE. Yes, I said the 2nd. Yes.

Mr. SMITH. The 1st was, I think, the first day it was sold.

Mr. LANCE. Yes.

Mr. SMITH. It is not unusual for stock to be sold at the end of a quarter. After we have our earnings call the window opens up. We encourage those who are going to sell, sells early in the window. The window is open for about 30 days. They sell as early in the window as possible and that is what occurred here.

Mr. LANCE. You believe that this stock was sold merely as a matter of course as would be true in any other quarter?

Mr. SMITH. Yes.

Mr. LANCE. You do not believe it was based upon knowledge known by these gentleman related to the breach?

Mr. SMITH. Congressman, I have known these individuals, some of them up to 12 years. They are honorable men. They are men of integrity. They followed due process. They went through the clearance process through the general counsel. I have no indication that

they had any knowledge of the breach at the time they made the sale.

Mr. LANCE. Did you have knowledge of the breach at that time?

Mr. SMITH. I did not, sir.

Mr. LANCE. Weren't you warned well in advance of this that there was suspicious activity?

Mr. SMITH. I was notified on July 31st in a conversation with the chief information officer that there was suspicious activity detected in an environment called the web portal for consumer dispute. No indication of a breach.

Mr. LANCE. That was prior to the sale of the stock; is that accurate?

Mr. SMITH. The 31st of July, but there is no indication of a breach at that time.

Mr. LANCE. From my perspective as a layman the difference between a breach and suspicious activity is not one that I believe is particularly relevant. A breach might have technical connotations to it, but certainly you were aware of untoward activity prior to that date; is that accurate?

Mr. SMITH. No, Congressman, it is not. On the 31st we had no indication that documents were taken out of the system, what information was included. It was very early days. It took the forensic experts as I mentioned earlier from then until the 24th to start to develop a clear picture and that picture still changed the 24th because we heard just last night the additional announcement.

Mr. LANCE. Many calls have been received by Equifax at your call center since September 7th. Do you know how many calls have been dropped or missed due to staffing shortages or other issues?

Mr. SMITH. Congressman, I don't have the exact number, but as I said in my opening testimony I apologize for that startup. It was overwhelming in volume, overwhelming. I think I mentioned over 400 million U.S. consumers coming to a web site in 3 weeks. We went live in a very short period of time with call centers. Our two larger call centers were taken down in the first few days by Hurricane Irma. The team is committed and was committed to make the experience better for the consumer and I am told that each and every day the process is getting better.

Mr. LANCE. On August 22nd, you notified a lead director, Mr. Fiedler—I hope I am pronouncing that right—of the data breach, and the full board was informed later, I believe 2 days later. Why was there nearly a week between August 17th and August 22nd before members of the board were alerted?

Mr. SMITH. Congressman, the picture was very fluid.

Mr. LANCE. Fluid, fluid. What does that mean?

Mr. SMITH. We were learning new pieces of information each and every day. As soon as we thought we had information that was of value to the board I reached out to the lead director as you said, Mark Fiedler, on the 22nd, convened a board meeting on the 24th. Convened a second board meeting on the 25th and had subsequent board meetings routinely, if not daily in many cases, through as recently as last week.

Mr. LANCE. Thank you. And my time has expired, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman's time has expired and the chair now recognizes the gentlelady from California for 5 minutes.

Ms. MATSUI. Thank you, Mr. Chairman, and thank you, Mr. Smith, for appearing here today.

As many of my colleagues have highlighted, the events that led to this data breach and the actions that Equifax management took after the fact are very upsetting. It seems that many Americans are in a place of breach fatigue. But this latest event that potentially impacts nearly half of all Americans should light a fire under every member here and I think you have noticed that it has lit a fire.

We cannot follow the same script after the next inevitable data breach. That is one of the reasons why I am also supporting Congresswoman Schakowsky's Secure and Protect Americans' Data Act. And it is not as if this type of legislation is unprecedented. Forty-eight states have implemented laws that require consumers to be notified of security breaches.

And I am pleased that my home state of California was the first state to pass this kind of notification law in 2002. Today, if California residents' personal data is hacked, state law requires that they are notified in the most expedient time possible and without unreasonable delay. We must act to ensure that all Americans are subject to protections like this at the federal level.

Mr. Smith, because Equifax without doubt has the information of many California residents, the company is subject to the California data breach notification law. Can you please describe to me how Equifax complied with the state law? Were California residents notified of the breach as required?

Mr. SMITH. Congresswoman, I don't have the specific knowledge of the California law. I can tell you though that we worked as a team including with our counsel to help us ensure we were doing what was right for the consumer in the most expedient manner as possible. So we are aware of the requirements of the specific state laws, I just don't have the specific knowledge as it relates to the State of California.

Ms. MATSUI. So you also don't know, because the law also requires Equifax to submit a copy of the breach notification to the California attorney general, you don't know whether this was done?

Mr. SMITH. Congresswoman, I do not. But we can have our team follow up through staff if that would be helpful.

Ms. MATSUI. OK. In the context of this breach, if data that you hold is about me do I own it? Do I own my data?

Mr. SMITH. Could you please repeat the question?

Ms. MATSUI. In the context of this breach, if the data that you hold is about me do I own it?

Mr. SMITH. Congresswoman, we are part of a federally regulated ecosystem that has been around for a long time and it is there to help consumers get access with their consent to credit when they want access to credit.

Ms. MATSUI. Well, can you explain what makes data about me mine compared to what would make it someone else's?

Mr. SMITH. The intent, if you will, of the solution we have recommended, we implement, and are going live with in January of

2018, is in fact to give you as the consumer through this lock product for life, for free, the ability to control who accesses your personal information and who does not.

Ms. MATSUI. So at that point in time you believe that I own, I can say I own my data; is that right?

Mr. SMITH. You will have the ability to control who accesses and when they access your data.

Ms. MATSUI. OK. Could I ask you some further questions following along to what others have asked about, credit locks and credit freezes? Now limiting access to credit even for a short amount of time can have real financial consequences especially for low-income populations. How quickly will a file be able to be locked and unlocked and how will you ensure that speed?

Mr. SMITH. Congresswoman, thank you for that question. That is a great advantage of the product we are offering for free versus the freeze, which again came about in 2004 out of regulation, and there states dictate how quickly you can access to freezing and unfreezing your file and oftentimes that can take days if not weeks because we are mailing data back and forth to the consumer.

In this case, the intent is in January of 2018, on your iPhone, you can freeze and unfreeze your file instantly at the point you want it locked and unlocked.

Ms. MATSUI. So, and I recall that one of my colleagues asked whether a credit lock is the same thing as a credit freeze and you said it was; is that correct?

Mr. SMITH. As far as protection to the consumer, Congresswoman, it is. As far as ability to lock or unlock and freeze or unfreeze, a lock is far more user-friendly.

Ms. MATSUI. OK. So you currently offer a credit lock product now and you plan to offer this other one for free starting the end of January. Would a lock be more economical for you or would a freeze be? I am trying to get the sense of the difference, because I think there is a difference here.

Mr. SMITH. Yes, if I may one more time try to clarify. As far as protection they are the same. The lock you are getting that we offered to the consumers on September 7th gives you the same level of security you would get from a freeze or from the product that is going out in January. The difference is today's lock is browser-enabled; January's lock will be an app on an iPhone. And secondly, it will be instant on and instant off versus the freeze or today's lock.

Ms. MATSUI. OK. I have more questions but I know I have run out of time. Thank you.

Mr. LATTA. Thank you very much. The gentleman from Illinois is recognized for 5 minutes.

Mr. KINZINGER. Thank you, Mr. Chairman, and sir, thank you for being here today.

This is obviously a huge issue, 145 1A½ million people affected by this data breach. It is nearly half of all Americans. That is a failure on multiple levels. It is a failure to keep consumer personal information secure. It is a failure to appropriately respond to a breach and a failure to notify the public and much more. My constituents and the American people need not just answers but they

want assurances that they are not going to be financially ruined by this.

I do want to make a quick point. Mr. Luján asked you if the people that would be harmed by this would be made whole and you made a statement. And I understand that there is probably some legal and technical reasons for this, but you said I don't know if consumers were harmed. I just want to make the point that I think that idea that people are not harmed in this is ludicrous. Of course they are going to be harmed. Even if there is no financial harm that comes to them just even having this information exposed is a massive deal, but I feel that we are going to see bigger repercussions from that.

But let me say now, Mr. Smith, I was surprised to find out that Equifax initially included a requirement that consumers consent to a mandatory arbitration clause. Why did that happen? Why was that at the beginning part of the rollout?

Mr. SMITH. Congressman, thank you for that question and I want to clarify. The product offering that went live or the service offering on the 7th, it was never intended to have that arbitration clause apply to this breach. It was a standard boilerplate clause as a part of a product. As soon as we learned that that boilerplate term was applied to this free service, I think it was within 24 hours we removed that and tried to clarify that. That was a mistake and one of the mistakes I alluded to in my oral testimony about the remediation product on September 7th.

Mr. KINZINGER. So does Equifax require consumers to consent to arbitration with respect to any of its other products and if not is that information prominently disclosed to the consumer?

Mr. SMITH. Not as it relates to the breach, Congressman.

Mr. KINZINGER. Well, the question is what about any other products do you require consent to arbitration?

Mr. SMITH. Some of the consumer products we have there is an arbitration clause in there. It is a standard clause.

Mr. KINZINGER. What is the reason for that?

Mr. SMITH. I don't have that answer other than it is a standard clause.

Mr. KINZINGER. If you could get that to me that would be good. Your press release indicates that the company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases. What are Equifax's core consumer and commercial credit reporting databases and how are they distinct from the databases containing personal information that was subject to the unauthorized theft?

Mr. SMITH. Congressman, the area that was impacted here was a consumer dispute portal where the consumers would come in and they would dispute activity with us. As separate then a congressman had talked about, had the credit file in their hand. That is separate from the core credit data that consumers have in our database.

Mr. KINZINGER. So in essence, were there 145.5 million people that at one point had disputed credit issues then, if that was the—

Mr. SMITH. It is a portal they used and they could have been in that portal for multiple reasons. And we also by regulation have

got to keep data for extended periods of time, in some cases 7-plus years. So it is a lot of data for a lot years, but it is outside the core credit file itself.

Mr. KINZINGER. Which company, and I guess you kind of went into this, which company databases were accessed, but why wouldn't you consider that then—maybe this is a change now after this—why wouldn't you consider that to be part of the core consumer and commercial credit reporting databases?

Mr. SMITH. It is just the way we define it. The credit file itself is housed and managed in a completely separate environment from a database that consumers can come into directly. The core credit file itself is largely accessed by corporations, companies that we deal with versus consumers.

Mr. KINZINGER. OK. So I just want to make sure and you will have to forgive me, I am not an IT expert. So to get 145 million people's records in only the dispute database, I guess I am trying to figure out if—you didn't really answer the question in terms of were there 145 million people that have disputed at some point in time, half of Americans, or was there another entry somehow through that that went into other information? Maybe I just don't understand the IT part of this.

Mr. SMITH. The only entry was through the consumer dispute portal and that is a completely separate environment from the credit file itself. We also, as you might recall, house a lot of data for small businesses in America and that environment which is part of the definition that you were alluding to was not compromised either.

Mr. KINZINGER. OK. And lastly, are your core consumer or commercial credit reporting databases encrypted?

Mr. SMITH. We use many techniques to protect data: encryption, tokenization, masking, encryption in motion, encrypting at rest. To be very specific this data was not encrypted at rest.

Mr. KINZINGER. OK, so this wasn't but your core is?

Mr. SMITH. Some, not all. Some data is encrypted, some is tokenized. Some it is in motion, some is masked. There is varying levels of security techniques that the team deploys in different environments around the business.

Mr. KINZINGER. OK, thank you, sir. I yield back.

Mr. LATTA. Thank you very much. The gentleman yields back. The chair now recognizes the gentleman from California for 5 minutes.

Mr. MCNERNEY. I thank the chair for holding this hearing.

Mr. Smith, it is my understanding that the compromised information was due to an unpatched vulnerability in the web application framework Apache Struts? Besides the company's online consumer dispute resolution portal, does Equifax have any other portals that use Apache Struts?

Mr. SMITH. No, sir. This was the environment that had deployed Struts.

Mr. MCNERNEY. All right. That was a simple answer. You might need to restart my time. In addition to Equifax's credit monitoring and reporting services, the company has Equifax for business offerings and in this capacity operates as a data broker. As a part of these services the company collects large amounts of data about

consumers without consumers having any knowledge of this happening. Was this information compromised in the breach?

Mr. SMITH. I think I understand your question, but could you repeat that one more time, please, so I get it right?

Mr. MCNERNEY. OK. Well, you are familiar with the Equifax for business offerings?

Mr. SMITH. Yes. We do have product offerings and solutions for small businesses, medium sized businesses and large business across the country, correct.

Mr. MCNERNEY. Right. Was information from Equifax for business also compromised in the breach?

Mr. SMITH. No, Congressman, it was not. It goes back to the question earlier on as part of our, what we call our core credit data. It was not compromised.

Mr. MCNERNEY. Well, in your testimony you noted that "throughout my tenure as CEO of Equifax we took data security and privacy extremely seriously and devoted substantial resources to it." Could you tell us about what investments Equifax made in cybersecurity during your tenure?

Mr. SMITH. Yes, Congressman, I can. When I came to the company 12 years ago we had virtually no focus on cybersecurity. At that time cybersecurity was not as sophisticated as it today. We have gone from the environment to a team now of over 225 professionals focusing each and every day on security around the world.

Mr. MCNERNEY. So what timeframe is that?

Mr. SMITH. That was from the time I started 12 years ago.

Mr. MCNERNEY. So you say that you hired up to 250 personnel to fix the issue?

Mr. SMITH. I did not, the team did. I didn't hire them, sir, but we now have a staff of 225 cyber or security experts around the world. We made substantial investments over that timeframe. In the last 3 years alone we have invested approaching a quarter billion dollars in security. There is an IBM benchmark. It says financial service companies who tend to be best in class spend somewhere between 10 and 14 percent of their IT budget in security.

Mr. MCNERNEY. Well, the company was notified of the vulnerability in the Apache Struts system days before the attack occurred.

Mr. SMITH. Yes. We were notified by Department of Homeland Security in March of 2017.

Mr. MCNERNEY. And the attack occurred after the notification?

Mr. SMITH. Yes.

Mr. MCNERNEY. So was there a human failure? How could 250 professionals that are designed and hired for that purpose let a breach like that happen after they were notified?

Mr. SMITH. Yes, Congressman. What happened and it was in my oral testimony was the notification comes out. We had a communication process in place. I described it as a human error where an individual did not ensure communication got to the right person to manually patch the application. That was subsequently followed by a technological error where a piece of equipment we use which scans the environment looking for that vulnerability did not find it.



Mr. MCNERNEY. You mentioned that in your opening testimony. That seems like a lack of competence or a professional error of some kind. What did you call it?

Mr. SMITH. I described it as a human error and a technology error, and I apologize for that but that is what happened.

Mr. MCNERNEY. OK, moving on. Do you believe that the FTC has an important role in protecting consumers from future data breaches? How much of a role should the FTC be playing at this point given what has happened?

Mr. SMITH. I think there is a role for the business to do more, industry to do more. We talked about earlier this concept of offering the consumer the ability to control their data and lock and unlock when he or she so choose. And if there is particular legislation that arises out of this horrific breach, I am sure you would find the management at Equifax and the industry willing to work and cooperate with the regulators.

Mr. MCNERNEY. Well, the reason I am asking is the Federal Trade Commission is an enforcement body, but it doesn't have any rulemaking authority. And do you think the FTC should have rulemaking authority? Do you think it would have made a difference or do you think it will make a difference in the future or do you have an opinion?

Mr. SMITH. I have no opinion.

Mr. MCNERNEY. Well, my final question then is how long will individuals be vulnerable to identity theft problems due to this breach?

Mr. SMITH. We, Congressman, offered five different individual services, as you may or may not be aware, effective September. One is the ability to monitor your credit files from all three of us for free, another is to lock your file, another is a dark web scanning product.

Mr. MCNERNEY. That doesn't answer my question. How long are we going to be vulnerable? How long are we going to—our social security numbers are out there. This is forever, right?

Mr. SMITH. Unfortunately, the number of breaches around a social security number has been on the rise as you know, and many even this year. So there is another thought and that is, do we think about how secure, really, is an SSN and is that the best identifier for consumers going forward?

Mr. MCNERNEY. Thank you, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman's time has expired and the chair now recognizes the gentleman from Kentucky for 5 minutes.

Mr. GUTHRIE. Thank you, Mr. Chairman.

Thank you for being here, Mr. Smith. We appreciate you being here to testify. And there is a medical hearing going on upstairs, so I have been back and forth so I will try not to double a question. But when I was here earlier and a lot of people have asked, a lot of us wondered, you know, July 31st was the suspicious activity and then it seemed the activity or the notice in the board was about 3 weeks later, August 24th and 25th.

And so not to repeat before, I heard you say that it was suspicious activity and therefore you didn't realize it was a breach and then the action took place 3 weeks later when you did. Looking

back now, knowing how colossal this is and how big it is, would you have done different? So from July 31st to August the 24th, what would you have done different that didn't happen or Equifax didn't do?

Mr. SMITH. Congressman, that is an appropriate question. To be honest, time for reflection will come. There has been no time for reflection. This has been a team of people including myself working around the clock for the last 6, 8 weeks trying to understand the forensics, trying as best we could to stand up an environment to offer consumers services to protect themselves. There will be an opportunity where I will have the time to catch my breath and reflect. I have not had a chance to do so now.

Mr. GUTHRIE. Thank you and I appreciate that. Well, 1.9 million Kentuckians were exposed in this hack. And one of the questions we have about the process that Equifax underwent to help people determine that and one was setting up a new web site, not just a portal within your web site, for consumers to visit. And was that an appropriate response? I know there were some issues with getting on to the web site. And the question is were you part of the deliberation and why did you choose to set up a new web site that seemed to cause issues as opposed to just doing a portal on your current web site?

Mr. SMITH. Congressman, good question. It was strictly due to the sheer volume of incoming visitors that we had expected. The traditional web site that we would use to interact with consumers services a total of maybe 7- to 800,000 consumers at any one given point in time over a period of time. I mentioned in my opening comments earlier, this new microsite as we call it that we set up had a capacity to surge to much higher levels. We had some 400-, and I think it was, 20 million consumers come to visit us in the first 3 weeks on that web site. Our traditional Equifax web site could not have handled that volume on day 1.

Mr. GUTHRIE. OK. According to reports, many consumers weren't able to determine with certainty if their information was breached. So why was Equifax unable to provide clarity or certainty on whether individuals' information was breached?

Mr. SMITH. When you went to the web site, Congressman, and you typed in six of your nine digits of your social security number, if it was likely that you were breached it would say something along the lines of it looks like you may have been compromised or breached as opposed to it is definite that you have been breached, and that is because it was six digits versus nine. The point is we offer these five different services to every American. It didn't matter if you were compromised or not, every American was offered the same services.

Mr. GUTHRIE. So, and just going forward, because we have to also do an analysis and so what we are going to do as a legislative body going forward to protect the American people. And what your business does and what people in your business do are important is when you can sit down at a car dealer, and I think you kind of mentioned earlier, walk away with a car that afternoon because somebody can check that you are creditworthy, and so having those types of services are available.

So what steps is Equifax doing to rebuild the confidence? People aren't confident that their information is flowing out there. But the ability to be able to access credit almost immediately if you have the proper credit is something that your services provide, but the risk is having all that information in one place plus the convenience of what your type of business offers. So what you doing to rebuild or how can people be confident that this can go forward?

Mr. SMITH. Congressman, that is a really good question. And we are a 118 year old company and we have done a lot of great things for consumers over those 118 years. We take being a trusted steward seriously. So step one is to make sure we think more holistically, broadly, about steps we can and have taken to make sure we are more secure today than we were at the time of the breach.

Second thing we could do is offer these services to consumers we offered on September 7th to make sure they are protected. And third is to launch this whole paradigm shift effective January of next year which is to put the power of the control of the consumer credit in the consumers' hands, not our hands.

Mr. GUTHRIE. Thank you, and that would be helpful. So I appreciate that and now my time is expired. I yield back.

Mr. SMITH. Thank you.

Mr. LATTA. Thank you very much. The gentleman's time has expired. And pursuant to committee rules we will go with the members on the subcommittee by order of appearance and then after that the non-subcommittee members. So the chair would recognize the gentleman from Florida for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it.

Mr. Smith, one of my constituents accessed Equifax's web site, [equifaxsecurity2017.com](http://equifaxsecurity2017.com), to determine if they were affected. They informed me that whether you submit your own identifying information or whether you submit a random name and social security number you get the same message that you may be affected. What course of action should consumers who haven't received correspondence yet as to whether they are affected or not, what is the course of action? And if they were affected what are the next steps?

Mr. SMITH. Congressman, it is my understanding that those who have gone online to register and that were not notified immediately that that backlog is completely now drained, if you will. So if you are trying to sign up for the service, if I understand your question correctly, you have now been notified.

Mr. BILIRAKIS. OK. I understand that Equifax currently is waiving fees to freeze and unfreeze your credit. How long is that exemption going to stay in place because it is so very important?

Mr. SMITH. It is important. Congressman, we have announced on September 7th the ability to lock and unlock your file at Equifax for free for 1 year from the time you sign up. We have also announced on a product we have been working on for quite some time, effective in January of 2018, the ability to lock and unlock your file with Equifax for life for free. That will be the next generation of the lock that we offered in September.

Mr. BILIRAKIS. OK. As CEO, what level of involvement did you have with regard to the data security and data protection?

Mr. SMITH. Yes. The—

Mr. BILIRAKIS. Obviously, the buck stops with you. I understand that. But what level of involvement did you have?

Mr. SMITH. So data security reported to a direct report of mine, my general counsel, and I would have active involvement with my general counsel, with the head of security, routinely throughout the year.

Mr. BILIRAKIS. OK. What responsibilities did Ms. Mauldin, again the chief security officer at Equifax at the time of the breach, have with respect to data security, data protection, and data breach notification? What were her responsibilities?

Mr. SMITH. Those were core to her responsibilities. She was the head of cybersecurity and physical security in all 24 countries that we operate.

Mr. BILIRAKIS. How many briefings did you have with Ms. Mauldin between March 8th and July 29th of 2017? How many briefings?

Mr. SMITH. I don't recall. We had, as a congressman asked earlier, there are routine meetings which we go through security strategy, security quarterly reviews, investment decisions required for security, but the actual number of times in that timeframe I don't recall.

Mr. BILIRAKIS. OK, so say a half dozen, a dozen?

Mr. SMITH. That would be a guess, I don't know.

Mr. BILIRAKIS. It would be a guess. More than three?

Mr. SMITH. If it is important to you, Congressman, we can find that information.

Mr. BILIRAKIS. Give me that information, I appreciate that. What responsibilities did Mr. Webb, the chief information officer at Equifax at the time of the breach, have with respect to data security, data protection, and data breach notification?

Mr. SMITH. Directly, none, sir. He was expected obviously as the head of technology to work closely with the head of security, but the security function was a separate function. But you can't do security without IT, you can't do IT without security.

Mr. BILIRAKIS. How many briefings did you have with Mr. Webb, again between March the 8th and July 27th of 2016?

Mr. SMITH. If I may just clarify again, on March 8th is when the CERT came out saying there was a vulnerability in Apache Struts. I was not even notified to put it in perspective that there was an incident and didn't know what the incident was until July 31st. So the number of meetings I would have with Dave Webb would not have been related to this incident.

Mr. BILIRAKIS. All right, Mr. Chairman. Thank you, I yield back.

Mr. LATTA. Thank you very much. The gentleman yields back and the chair recognizes the gentleman from Indiana for 5 minutes.

Mr. BUCSHON. Thank you, Mr. Chairman. Thank you for being here. And again I was at the Health Subcommittee hearing too, so I am back and forth. Sorry about that.

But is it possible for people who never signed up or used Equifax directly could have been impacted by the breach?

Mr. SMITH. Yes, Congressman.

Mr. BUCSHON. OK. So how does Equifax get the information on people who have never directly associated with Equifax at all? I mean I am not familiar with that.

Mr. SMITH. Yes. We get it from banks, telecommunications companies, credit card issuers, so on and so forth.

Mr. BUCSHON. So just like, when we go to apply for a loan they send you the information because they want to get a data, they want to get the information on my credit rating, for example?

Mr. SMITH. Correct. As I define it we are part of the federally regulated ecosystem that enables banks to loan money to consumers.

Mr. BUCSHON. Right. So it is up to the banks at that point to notify the individual which credit agencies they are utilizing to assess their credit risk, or is it up to the credit agencies?

Mr. SMITH. Traditionally, the contributors of the data in that case, Congressman, the banks, would give their data to all three. That is the benefit of the system is you get a holistic view of an individual's credit risk.

Mr. BUCSHON. Yes, and my point is I guess because a lot of people I talk to back in Indiana, southern Indiana, have no idea who Equifax is, right. And many of those people have applied for home loans and other things and matter of fact probably at some point you have their information, but they just, they may or may not have been notified who had sent the information to them, probably the bank or other agency.

And that is just something I think that is also maybe an issue that people don't understand or have not been told who is being used to assess their credit risk, and hence something like this happens they have no idea whether or not their information has been compromised.

Mr. SMITH. I understand your point.

Mr. BUCSHON. Yes. I also have a lot of constituents in rural and lower income areas that may or may not have access to the internet and WiFi. The penetrance of that it is interesting depending on where you are of people who actually have WiFi and the internet is not as high as you might think in rural America, but some of those people still have probably applied for loans and other things where their information could have been acquired by your company.

How are you notifying all of those people other than saying that you have a web site? And you may have already answered that and I apologize if you have. But that is important because again the penetrance of people having access to the internet may be not as high as you think when you come out to like rural Indiana and other areas.

Mr. SMITH. Yes. Coming from Indiana I understand rural Indiana.

Mr. BUCSHON. There you go.

Mr. SMITH. Congressman, we have set up the web site that you mentioned at a press release across the country. We have also set up for those that don't have access to the web, to the internet, call centers. We have staffed up. We have gone from some 500 call center agents to over 2,700. So—

Mr. BUCSHON. I guess that is, again, I understand the call centers and all that. I knew you had done that. But I guess that is again making the assumption that people have watched the news

and know that there has been a breach and that they are proactive in trying to find out whether they have been involved or not.

Is there any, other than a passive way for them to find out, is there anything proactive from Equifax's point of view that might notify them that their data may have been compromised?

Mr. SMITH. Well, in many states there is local requirements, state requirements to take out advertisements in newspapers and so forth. We follow those. One indication I did mention earlier, it may or may not help those in rural Indiana, but the visibility this has gotten is extremely high. I mentioned 400 and some odd million consumers had come to our web site, so it has gotten the press.

Mr. BUCSHON. And probably after today it will be, maybe more people will know. So thank you for answering those questions. Like I said, my main concern is that my constituents understand whether or not their data has been compromised and then what are their options going forward. You have outlined most of those things today. I am not going to ask you that again.

But I do think it is important to recognize that you know, although they are important, passive ways to have people become aware of their data may be compromised is one approach, but also actively informing people proactively might very well be important in certain areas of the country. Thank you, I yield back.

Mr. LATTA. The chair now recognizes the gentleman from Texas for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman, and I apologize. We have a Health Subcommittee upstairs and I appreciate it. That is not to take away the importance of this hearing. I want to thank you and our ranking member for setting it.

We are here to discuss one of the worst and most impactful hacks that we have seen. It is a breach that was entirely preventable due to a level of negligence that in some industries may be considered criminal. The credit reporting industry is infamously unforgiving and it is an industry that helps perpetuate the cycle of poverty. Agencies like Equifax force those with lower credit scores to pay more money for loans and mortgages, less than perfect credit scores can even result in higher rates for products that they don't require credit like our auto insurance premiums. These people who have a harder time paying back higher interest rates make it more likely they won't be able to pay their debt back on time and will hurt their credit further. Yet Equifax and the rest of the credit reporting industry expect forgiveness for breach after breach, lobbying Congress for even less liability.

When restaurants fail regular health inspections they are routinely shut down for violations. They are shut down even if problems haven't yet occurred as a consequence of their violations. It isn't clear to me why Equifax, who is beyond that point, should be allowed to continue operating when they have failed spectacularly at their core business and endangered the public. In the next couple months, Senate Republicans may repeal the Consumer Financial Protection Bureau's arbitration rule thus allowing companies like Equifax to put clauses in their fine print forcing individuals into arbitration agreements instead of class action agreements where they stand a chance of being able to cover some of their loss.

But it should be clear to us by all that is now not the time to roll back consumer safeguards in the financial industry and I support my colleague and our ranking member Congresswoman Schakowsky's Secure and Protect Americans' Data Act. I look forward to hearing what our witness has to say.

Mr. Smith, ID theft protection companies have seen a big jump in business and share price since the breach of your company including LifeLock who has reported a tenfold increase in enrollment for their credit monitoring and other services. LifeLock has a contract to purchase credit monitoring services from Equifax, meaning that every time someone signs up for LifeLock protection from the impact of Equifax' data breach they again involuntarily sign up for Equifax to provide those services and Equifax makes money on that breach. What is the value of that contract that LifeLock has with Equifax?

Mr. SMITH. Congressman, I don't recall what that is. But at the same time, those same consumers have the ability to come to us directly and get free product.

Mr. GREEN. OK. If it is available I would hope you would send it and share it with the committee. Mr. Smith, an Equifax report marketed to its business customers says that leading lifestyle databases available commercially offer hundreds of response segments covering almost every conceivable aspect of how consumers live and what they spend their money on and what interest they have.

Can you tell us on as granular level as possible what the sources are for that data for every conceivable aspect of a consumer's life?

Mr. SMITH. Congressman, I am not quite sure what you are referring to. We are not a data provider in the area of behavioral analytics, behavioral data, social media data, so I am not quite sure what you are referring to.

Mr. GREEN. Well, I have a lot of constituents who are concerned about, for example, they say oh, I don't need to worry about this breach, I haven't applied for credit for 10 years. But that is not always the case because these hundreds of millions who are released, maybe they bought a car 20 years ago and that data still goes forward, I assume.

Mr. Smith, Equifax customers are businesses who purchase data and credit reports on consumers. The American public is essentially Equifax's product. How many times per year on average does Equifax sell access to a given individual's credit file to a potential creditor and how much do they make every time they sell it?

Mr. SMITH. If I understand the question, Congressman, we take the data that is given to us by the credit ecosystem of the U.S., add analytics to it, and then when a consumer wants credit again through credit card, home loan, a car, the bank then comes to us for that data and for the analytics and we charge them for that.

Mr. GREEN. OK. Well, the question was how many times does Equifax receive payment for that individual credit file? If my local car dealer contacts Equifax and so they pay a fee to Equifax for that information?

Mr. SMITH. Yes, Congressman. If you as an individual want to go to that car dealership and get a loan for a car they come to us or our two competitors, and when they take your data, access your data we do get paid for it.

Mr. LATTA. Pardon me. The clock wasn't started right. You have about 15 seconds.

Mr. GREEN. I am sorry?

Mr. LATTA. You have about 15 seconds. The clock didn't start up on you, so you have 15 seconds.

Mr. GREEN. Oh, OK. Oh, I thought I just had a perpetual time.

Mr. LATTA. No.

Mr. GREEN. Mr. Chairman, I just have one more question. The products that Equifax are so far providing victims of the breach do not include anything they won't need if it weren't for Equifax's laxes on their data. You, however, made more than \$69 million in 2016. And so, but that is the concern that this committee has and I know we have for all our constituents.

And I thank you, Mr. Chairman, for your time.

Mr. LATTA. Well, thank you very much. I appreciate the gentleman's questions. And the chair now recognizes the gentleman from Oklahoma for 5 minutes.

Mr. MULLIN. Thank you, Mr. Chairman.

Mr. Smith, what is your current job?

Mr. SMITH. I am retired.

Mr. MULLIN. You are retiring. Are you still getting paid by the company?

Mr. SMITH. No, sir.

Mr. MULLIN. So you are fully retired and so you have no affiliation at all with the company? You are not on as a contractor or as—

Mr. SMITH. No, Congressman. What I agreed to do because I love this company, I spent 12 years with 10,000 people trying to do the right thing, is I told the board it was right for me to step down and have new leadership, take this company in a new direction. So when I retired I agreed to work for as long as the board required, for free, to help make it right for the consumers. So the affiliation is to do free work with the board of directors and the interim CEO.

Mr. MULLIN. So you are not getting paid in any manner, not through any type of shares, stocks, anything?

Mr. SMITH. Nothing. The day I announced my retirement that ended.

Mr. MULLIN. Do you still own stock in the company?

Mr. SMITH. I am sorry?

Mr. MULLIN. Do you still have stock in the company?

Mr. SMITH. Oh, yes.

Mr. MULLIN. Have you sold any of it?

Mr. SMITH. I have been there for 12 years. Yes, sir.

Mr. MULLIN. In recent, since this has become aware to the public?

Mr. SMITH. During this breach?

Mr. MULLIN. Yes.

Mr. SMITH. Oh, No, sir.

Mr. MULLIN. Are you aware of the individuals that have?

Mr. SMITH. Yes. There are three individuals who reported directly to me while I was their CEO.

Mr. MULLIN. That sold stock?

Mr. SMITH. Yes. One, yes, and all three of them are men I have known, I mentioned earlier, for a number of years. Two for almost



12 years and one for 3 or 4 years and they are men of high integrity.

Mr. MULLIN. Did they sell it before this went public?

Mr. SMITH. Yes. As I said before, we went public with this knowledge on September 7th.

Mr. MULLIN. And when did they sell their stock?

Mr. SMITH. August 1st and 2nd.

Mr. MULLIN. So after the breach?

Mr. SMITH. No, sir. The timeline of the end of July, 29th and 30th and notification on the 31st of suspicious activity, at that time 1 or 2 days prior to their selling there was no indication of a breach.

Mr. MULLIN. So what would cause them to sell it?

Mr. SMITH. As a what we call a Section 16 Officer, there is a limited window in which they can sell. It tends to be right after the earnings call for no more than 30 days, so this is a natural process. The window opened after the second quarter window, second quarter call.

Mr. MULLIN. In your opening statement you had mentioned that there was an error in the portal and it was 3 weeks before you were notified of a breach?

Mr. SMITH. If I can clarify?

Mr. MULLIN. Yes.

Mr. SMITH. There was a software, it is called an open source software that was deployed in this environment, this consumer dispute portal.

Mr. MULLIN. Right.

Mr. SMITH. We never found a vulnerability, didn't patch that vulnerability. That was the issue.

Mr. MULLIN. So who was in charge overseeing that? Who was supposed to be watching those portals for you?

Mr. SMITH. Ultimately me.

Mr. MULLIN. I know. Ultimately you, I get that. But who did you have hired that was supposed to watch that?

Mr. SMITH. There was on the vulnerability side, there was the—

Mr. MULLIN. Do you have a department that is dedicated to this?

Mr. SMITH. Yes. There is a chief information officer who was ultimately responsible. He was—

Mr. MULLIN. Is that person still over that department?

Mr. SMITH. No, sir. He is gone.

Mr. MULLIN. He is gone. You said you put in, once you were made aware of the breach you put in four plans of action, right. The first one was, do you remember?

Mr. SMITH. Notification.

Mr. MULLIN. Notification. The second one was a call center. The third one was increased cyber attacks, preparing for that. The fourth one was coordinating with law enforcement. I am also or was CEO, not on a company the size that you have but from the companies that my wife and I have had and we have protocols put in place of what could happen. We know cyber attacks happen, you hear it every day on the news.

These four things that you named were common sense, things that should have been put in place to begin with. It should have

been the fire alarm. You are in that world. This should be on the side of the wall where you pull the handle and it immediately goes into place. How was it that it was just now thought of that you needed to have four common sense principles put in place on how to react to something in a world where we knew you were vulnerable at?

Mr. SMITH. We have protocol, team followed protocol. This is well known what to do. From hiring a cyber forensic expert we knew what to do, we have done it before. Engaging a world-leading cyber arm of a law firm, we knew what to do. These are all protocols that they knew what to do.

The one thing, Congressman, it is not a switch on a wall. It is the ability to stand up the environment we had to stand up—

Mr. MULLIN. It took a long time to stand up and that is the issue we have here is you are on the leading front of this. And the four things that you identified to me, I don't mean to simplify it by saying a switch on a wall, but these protocols should have already been put in place and you should have been on a react much, much sooner than what took place. And with that I am sorry. I don't mean to cut you off, but the chairman has indulged me longer than what he should have and I appreciate your time. Thank you, Mr. Chairman.

Mr. LATTA. Thank you very much. The gentleman's time has expired and the chair now recognizes the gentlelady from California, Mrs. Walters, for 5 minutes.

Mrs. WALTERS. Thank you, Mr. Chairman.

Mr. Smith, before I get to my question I just want to say that on behalf of the 15 million Californians whose information was exposed, we expect better. Your business model was based on collecting and maintaining the most sensitive information on folks and you let us all down and that happened on your watch. And from my briefings it appears that this could have been and frankly should have been prevented.

Now Equifax's business model depends on gathering consumer information, repackaging it, and selling it. Equifax has set up a web site in which consumers can enter information to determine if they are at risk and sign up for credit monitoring and credit lock. To participate, a person has to give Equifax the same type of personal information, including social security number, which Equifax put at risk in this breach. I want to know what Equifax is planning to do with this information besides offering credit monitoring and credit locks. Can you ensure me that Equifax will not plug this information back into its core business operation and sell it to its lenders?

Equifax should not benefit from the situation and I want to know that Equifax is going to wall off this information and guarantee that the company will not profit from this situation.

Mr. SMITH. Congresswoman, thank you for your comments. And as I mentioned in my written testimony and my oral testimony, I have said throughout the morning and I will say again today, as the CEO it was under my watch. I am responsible. I am accountable and I apologize to all of your consumers in California.

The intent of this offering that we are giving to your constituents in California and to consumers across the country is in an environ-

ment where we are not going to sell other products. It is to come there and be service protection of the five offerings that you had mentioned, not to sell and take your data and monetize that. It is to take and protect you with these five services.

Mrs. WALTERS. Equifax's breach notification web site uses a stock installation of WordPress. This causes me a lot of concern because it seems to have insufficient security for a site asking people to provide part of their social security number. Can you assure me that this web site is secure and will not further endanger the personal information of my constituents?

Mr. SMITH. Congresswoman, we took what we believe was the right amount of time working hastily from late August to going live on the 7th. One of the four work streams the Congressman from Oklahoma mentioned was ensuring we were prepared for what was going to be increased cyber attacks as told to us by our forensic examiners. And one of the first things we did was ensure that the web site we were bringing consumers to, to get these free services, was as secure as possible. So that was one of our top priorities.

Mrs. WALTERS. OK. And finally, my last question is how many U.S. consumers have enrolled in the credit monitoring service TrustedID? I will just finish here, because I know multiple people who have enrolled including my immediate family and they were told that they would receive an email to complete the process. After days of waiting they have not received an email and wanted to know what the delay is in processing this protection and when will they be able to complete the process to help protect their information?

Mr. SMITH. I understand the question and I mentioned earlier that over 400 million consumers have come to the web site. I would assume we don't have 400 million consumers in the country so a number of them came back multiple times. But it is a lot of volume. Number two, I was told in the last few days that the backlog waiting for those emails has now been fulfilled, had been drained. As you come into the system it is a more immediate response, so the team seems to have made great progress in the last couple weeks.

Mrs. WALTERS. OK, thank you. And I yield back the balance of my time.

Mr. LATTA. Thank you very much. The gentlelady yields back and the chair now recognizes the gentleman from Pennsylvania for 5 minutes.

Mr. COSTELLO. Thank you, Mr. Chairman. I have heard from hundreds of constituents in my congressional district. There are approximately 5 1A½ million in Pennsylvania. I have reviewed each and every one of the constituent stories that I have received.

And among my growing concerns, your baseline security practices leading up to the breach, the company's awareness of the breach developments and relevant timing, how consumers can get assistance in securing their accounts, how reliable the recovery efforts are in the wake of the breach, and the path forward long term for consumers' personal information and making sure they are safe despite the breach.

And it is this last one that is so particularly angering because it is going to potentially be so destructive to hundreds of millions

of Americans what might happen to them in the years to come. And as the head of the company and throughout the company, the culture of that company has to know how predictable the damage can potentially be.

And so I ask you, is it not predictable how bad it might get for the individuals who have been compromised in terms of how much damage could be wrought upon them individually in the years to come?

Mr. SMITH. Congressman, let me start by saying that like you I have talked to constituents, consumers across this country who have been impacted. I have personally read letters from consumers complaining and voicing their anger and frustration, so I know what you were seeing back home in Pennsylvania.

Mr. COSTELLO. See, I think the anger is going to be multiplied thousands of times when something actually happens. So when you talk about how predictable some of this is, the rollout of the call centers and the second rollout and the third rollout, it has to be predictable how massive this is and what would need to be put in place from a protocol perspective in order to address what is coming.

And the slow rollout and how poor it was done to me is just inexcusable. I mean you have to have departments dedicated to dealing with this potential and it doesn't appear to me as though that was planned. Or if it was planned it was planned extremely poorly.

Mr. SMITH. I understand your point, but it requires a little more color. We went from 500 call center agents to a need of almost 3,000. Properly handled call center agents to handle consumer calls took time. We did the best we could in a short period of time to ramp those up. I mentioned in my opening comments two of our larger call centers in the first weekend—

Mr. COSTELLO. I understand, the hurricane.

Mr. SMITH [continuing]. Taken out by Hurricane Irma. We were not prepared for that kind of call volume.

Mr. COSTELLO. How couldn't you be? How couldn't you be?

Mr. SMITH. It is not our traditional business model. Our traditional business model is dealing with companies, not 400 million consumers coming to the web site.

Mr. COSTELLO. But your business model has a couple hundred million customers, so on a breach of this scale obviously you are going to have at least that number and probably twice that amount calling, inquiring as to whether or not they are subject to the breach and that wasn't done.

Mr. SMITH. Congressman, the difference is again the primary business model we have is dealing with companies, not with hundreds of millions of consumers. We did the best we could to react as quickly as we could. I had mentioned that the service is getting better each and every day. We have listened to consumers' feedback and tried to make changes to the web site, we have made changes to the call center.

Mr. COSTELLO. You are familiar with the Safeguards Rule that is essentially what you operate under?

Mr. SMITH. Yes.

Mr. COSTELLO. How often does a forensic consultant issue a letter or a certification or a law firm issue a certification that they feel your protocol is in compliance with the Safeguards Rule?

Mr. SMITH. We are in compliance. I am not sure how often that is actually communicated, is you are saying communicates with us?

Mr. COSTELLO. How would you know that you are in compliance then? Because if you said you followed protocol and protocol led to this, then it is very difficult for me—that calls into question whether the Safeguards Rule is sufficient enough. Because if you are saying you are in compliance with it and you followed protocol and this still happened that unearths a whole other set of questions.

Mr. SMITH. Again the speed of reaction and the scale of the reaction was unprecedented for. I am not making any excuses.

Mr. COSTELLO. Yes. But there is a corporate governance issue here as I see it and that is your board of directors gets together, you are CEO. You have a chief information officer, you have a chief security officer and at least once a year and probably quarterly you have, I presume, outside forensic consultants doing this stuff every single day from you on retainer. And the speed at which you have to do this just to run your company operationally you don't ever stop. It is obviously ongoing and persistent.

And it just seems to me that through insurance policies, through reporting to your board, through your board wanting to make sure that they are doing their job that you are going to be looking for certifications from your outside forensic consultants doing audits to say yes, you are doing good. You are doing good. Here are the new threats. Here is how we are updating. That is the kind of information I think would be extremely helpful that we have not received any information from today.

But I would ask you since I am well over my time that I would like to know how often your board asks you to certify whether or not you are in compliance and what is that protocol and when was the last time you updated that protocol? You said you have complied with protocol. When was the last time that was updated?

Mr. SMITH. I understand your question. We will get you that information.

Mr. COSTELLO. Do you yield back after you are already well over? I yield back.

Mr. LATTA. Your time is expired, how is that? The chair now recognizes the gentleman from Georgia—I am sorry. The gentleman from New York, 5 minutes.

Mr. TONKO. Thank you, Mr. Chair. Americans should know their sensitive personal information is safe. Their security is exposed when private companies including Equifax can collect their private information without their direct knowledge or consent, and it is why I am co-sponsoring Representative Schakowsky's measure, H.R. 3896, the Secure and Protect Americans' Data Act.

Mr. Smith, we are here today because months after the breach actually took place your company, Equifax, revealed that its for-profit business practices have exposed the highly sensitive personal information of some 145 1A½ million Americans and counting. Your data breach exposed a critical vulnerability in the American economy and the information security of the American people. Victims of this breach span every age group, every race, class, and

other demographic. They now face a lifetime at risk of fraud, identity theft, and other crimes as a result of the private data that you exposed.

I have many, many questions and allow me to be the conduit through which my constituents ask you, Mr. Smith, their questions. I will go first to Garance (ph.), a constituent, pointed out to me it would be wrong to call the victims of this breach Equifax customers. Most of them never asked to be tracked and judged by a private company with little public oversight or accountability. This is unacceptable. And he asks why he has been impacted in this manner. Any comment to Garance's question?

Mr. SMITH. Again, Congressman, I have read many similar letters and talked to people back home in Atlanta who voice that same concern. I can tell you this. Where a company has been around for 118 years, have 10,000 employees trying to what is right each and every day, I apologize to the individual who wrote you that letter. I apologize to America for what happened and we are going to try to make it right.

Mr. TONKO. My constituent Jason from Albany asked, Mr. Smith, did you to the best of your knowledge employ the best and most effective defense available to you to prevent this breach?

Mr. SMITH. A crisis never occurs if everything has gone right. In this case as I mentioned earlier we had a human error and a technology error. It wasn't because we were unwilling or unable to make the financial investments in people, process, or technology though.

Mr. TONKO. My constituent Tanya asks, how do I get Equifax to fix this without signing over my rights and what related costs will I, Tanya, be expected to pay over my lifetime?

Mr. SMITH. The five products we launched or the services we offered in September are all free. They are all spelled out in the press release that gives that individual significant protection. The most comprehensive change is coming in January of next year which is the ability for consumers to lock and unlock their data when they want and only when they want.

Mr. TONKO. And any related costs that she should expect to pay over her—

Mr. SMITH. Those services are all free.

Mr. TONKO. A number of my constituents would like to know, given that the sole purpose of credit agencies is to secure handling of consumers' confidential information which they spectacularly failed to do that why is this company allowed to continue to exist?

Mr. SMITH. We have a rich history of helping those who want to get access to credit to get access to credit. The company has done many great things to help those in the unbanked world who would never otherwise have access to credit because of what we do, bring them into the credit world.

Mr. TONKO. Constituent Lee from Albany asks, why are you using this gross misconduct to turn your victims into customers for a paid monitoring service that you will profit from?

Mr. SMITH. That is not the intent. Our intent is to offer those five services for free, followed by the sixth service, which is a lifetime lock for free.

Mr. TONKO. My constituent Karen asks why have you not notified each person whose data you compromised? Most never asked you to collect it and securely store their private information, so we are the representatives and why should they be responsible for your malpractice?

Mr. SMITH. Following the recommendation of those who advised us we did notify through the press release notifying the entire population, not just those who were victim of the criminal act but all Americans, to get access to these products and services for free.

Mr. TONKO. And my constituent James from Defreestville, New York asks why did it take you so long to announce the data breach and why shouldn't you be held responsible for every day of failing to report?

Mr. SMITH. I think hopefully my written testimony and my oral testimony and the dialogue we have had today has talked about the timeline in enough granularity to help that person understand what occurred from March through September 7th.

Mr. TONKO. And a constituent Stephanie from East Greenbush asks, do they know if the people were targeted or randomly picked? Why some but not others?

Mr. SMITH. At this point all indications are it was at random. It was not targeting of individuals specifically.

Mr. TONKO. I have exhausted my time, but let me assure you, Mr. Smith, I have many, many, many constituent questions that continue to pour forth and we are going to provide those after the hearing here and would expect that they would all be answered. And again thank you for your response. I yield back, Mr. Chair.

Mr. LATTA. Thank you very much. The gentleman yields back and the chair now recognizes the gentleman from Pennsylvania for 5 minutes.

Mr. MURPHY. Thank you, Mr. Chairman, for allowing me to sit in on this hearing. My fellow members have already asked a lot of questions, very important high level questions, but I want to take a few moments to dig a little more deeply into a few specific issues.

We now know that Equifax information security department ran scans that should have detected systems that were exploitable by the Struts' vulnerability but that the scans didn't detect any. Obviously at least one system was vulnerable. So if the scan wasn't properly configured to catch this vulnerability, in other words you missed a major breach, is it possible that it has also been improperly configured to detect similar vulnerabilities?

Mr. SMITH. I have no knowledge of that. I have no knowledge of that being the case.

Mr. MURPHY. But now you have to feed the information in these scans and it has to be complete and accurate information and this information apparently was fed in an incomplete way; isn't that true?

Mr. SMITH. Could you repeat the question, please?

Mr. MURPHY. In order to scan something a human has to feed it information, right?

Mr. SMITH. I am not a scanning expert, Congressman. My understanding is you have got to configure the scanner in certain ways to look for certain vulnerabilities.

Mr. MURPHY. Yes, but a lot of what is going on here is you are blaming, they say no humans are involved here, but configuring is done by a human being, isn't it right? And some inaccurate information got in there too. So if it was improperly configured to catch the vulnerability, is it possible it has also been improperly configured to detect similar vulnerabilities?

Mr. SMITH. I have no indication to believe that is the case.

Mr. MURPHY. We have also heard a lot about the web site Equifax set up to handle the consumer protection response at [equifaxsecurity2017.com](http://equifaxsecurity2017.com). As it has been pointed out, this looks like a web site that scanners would use for phishing. In fact, it was widely reported in the press someone switched two words and made it into phishing web site that looked almost identical. Luckily, this person was just trying to make a point, but I think that point is well taken.

You said earlier today that you set up this external web site because Equifax's own domain wouldn't be able to handle the sheer amount of traffic. Now why wouldn't your web site be able to handle this traffic? I mean it just doesn't make sense a company of your size and knowledge doesn't understand how to handle traffic for over a 100 million people. Don't you use an elastic cloud computing service that would have accounted for this traffic?

Mr. SMITH. Congressman, a point of clarification, if I may. This phishing site that you referred to was mentioned a few times today, was a error by an individual in the call center. My understanding is——

Mr. MURPHY. Well, let me get this other question though. OK, we have that established, but I want to ask this question though. Your own domain wouldn't be able to handle the sheer amount of traffic, but don't you use something like an elastic cloud that would allow for greater traffic?

Mr. SMITH. The environment the microsite is in is a cloud environment that is very, very scalable. The traditional environment that we operate in could not handle 400 million consumer visits in 3 weeks.

Mr. MURPHY. Well, I am going to come back to some of this stuff too. I want to come back to the issue of patching the March vulnerability. Now I know this has come up a few times, but I want to make sure to highlight this point since it is critical in understanding how this breach occurred here.

Our understanding is that fixing this vulnerability required more effort than simply installing a patch. But we also understand that when Equifax did patch the vulnerability it took less than 3 days to do so. So if the patch only took a few days to apply, why did Equifax fail to install it immediately after it was announced as critical?

Mr. SMITH. Patching takes a variety of time. I am not sure where you got the note that it is 3 days. Patching can take from days to up to a week or more to apply a proper patch.

Mr. MURPHY. Did you notify everybody it was going to take some time? Did you notify all your customers it was going to take some time? Did you notify people there was the risk of your trying to apply the patch?



Mr. SMITH. I know of no standard protocol that we would notify—

Mr. MURPHY. I didn't ask about standard protocol. I asked did you notify people.

Mr. SMITH. I have no knowledge that we would notify customers or consumers of a patching process.

Mr. MURPHY. So you didn't notify anybody that the patch was going to take place and in the meantime there was a risk that existed?

Mr. SMITH. I have no knowledge of need—

Mr. MURPHY. Did you notify other people—did other people and the executives of your company, were you aware of it?

Mr. SMITH. As I have said before I was not.

Mr. MURPHY. You were not aware that there was this problem with the vulnerability? You just told me it takes a few days or a few weeks, but you weren't aware that it existed?

Mr. SMITH. That is correct.

Mr. MURPHY. Well, let me wrap up with one final thought here. In your testimony you state that the breach occurred because of both human error and technological failures, or technology failures. So looking at the three features I just highlighted—the improperly configured scans, the poorly chosen web site, the lack of patching—these are not failures of technology. A human misconfigured the scan. A human selected the web site name. A human failed to apply the patch.

While I understand that cybersecurity is an immensely complicated field, we have dealt with this many times in this committee and sometimes flaws in technology we rely on are really to blame, but I also think it is important to be upfront about the causes of breaches like this. And if we continue to blame technology for human failures to provide inadequate cybersecurity, I think we are going to have a very difficult time improving our capabilities and preventing future cyber threats.

Mr. Chairman, I recognize I am out of time. We will see you again in my subcommittee.

Mr. LATTA. Thank you very much. The gentleman's time has expired and the chair now recognizes the gentleman from Maryland for 5 minutes.

Mr. SARBANES. Thank you, Mr. Chairman.

Mr. Smith, thank you for being here. You have been the president of the company for, CEO for 12 years; is that right?

Mr. SMITH. That is correct.

Mr. SARBANES. There is three things I think that the public is angry about. Certainly, as my colleague was indicating, we are getting a lot of messages and contacts, inquiries from our constituents across the country.

First of all, they want to understand. And you have tried to explain it today, but I am not sure it is going to be satisfactory why there weren't sufficient protections in place on the front end so that this kind of breach wouldn't happen in the first place given the sensitivity of the information that you are keeping in the company. The second thing is how quickly once a breach was discovered you came clean to the public and provided information on what was

happening. There seems to have been a delay there that concerns people.

The third is whether the services that you are now providing to people, you have enumerated to five or six free services that you are providing to people, whether that is going to be a sufficient assurance to folks going forward that their identity can be protected, that their information is safe and so forth. So you are trying to fix things now, but there is going to continue to be, I think, serious questions about all three of those things that I just mentioned.

I wanted to ask you about the kind of remedies that you have out there because there is some confusion. I got a question from a constituent who had purchased a monitoring service that would cover his family including a child under the age of 18. So first of all, can you tell me, it is possible for someone under the age of 18 to have their identity stolen. Is that correct as far as you understand?

Mr. SMITH. Is it possible?

Mr. SARBANES. Yes.

Mr. SMITH. As it relates to this breach?

Mr. SARBANES. Just generally. Identity, if certain information about a minor is divulged to some unscrupulous actor that can be used to steal the identity of that person.

Mr. SMITH. If someone has a social security number, at any age, can that be compromised? Yes. It could not be compromised in this case because this database they got into it is my understanding only was for those who had credit, credit active or inactive, and they have been in a credit environment.

Mr. SARBANES. OK. But my understanding is that when you provide a family service you are collecting information and holding information that includes the social security number of people who may be under the age of 18.

Mr. SMITH. I have no knowledge that under 18, not credit active, was compromised here. I can look into that.

Mr. SARBANES. OK.

Mr. SMITH. But I have no knowledge.

Mr. SARBANES. If that is the case, is this free service that you are providing going to cover any exposure or information that is related to a minor, as opposed to somebody who is over the age of 18, if you had information on that minor?

Mr. SMITH. I can look into that, Congressman. The intent of the coverage was to cover anyone in America who is in the credit system. So if you are under 18 and not in the credit system, I will check your one point which is on this concept called family plan that you are alluding to where you lock down consumers, you monitor consumers. I don't believe their social security numbers were in this system, but we can verify that.

Mr. SARBANES. Well, that is important because—

Mr. LATTI. If I could just interrupt. I think again we had a little clock issue. You have about 30 seconds left. Thank you.

Mr. SARBANES. OK. I think it is important because it may be that with respect to credit reporting the implications of this breach only attach to people that are 18 or older. But if you are holding information about minors like a social security number that is part of the portfolio of information you are getting from a family, for ex-

ample, particularly when the family has paid for this service, you are holding their social security number, so any breach that makes that information available outside of the arena in which it is supposed to be kept close creates vulnerability for that person.

It is not like we get a new social security number when we turn 18. So that is going to follow them all the way through and create some real risk for them. So I think that is a piece of this that we need to understand much better, and I want to thank my constituents for bringing that to our attention.

Mr. SMITH. I understand your point. To the best of my knowledge, that data is not included in the breach, but I will look into it.

Mr. SARBANES. Thank you. I yield back.

Mr. LATTI. Thank you very much. The chair now recognizes the gentleman from Georgia, 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman. And I want to thank you for allowing me to sit in on this today.

Mr. Smith, thank you for being here. I know it has been a tough day. It has been a tough past couple of weeks. I appreciate you being here and that is important. I am not going to apologize for my colleagues and their questions and their aggressiveness, if you will, because as you know people are upset and they are mad. You get it and I get it, we all understand it. But nor am I going to pile on, so I want to go a kind of different route, if you will.

One of the things that I have learned in the 2 1A½ years that I have been up here is to be very careful about my southern phrases, but one of my southern phrases has always been that you know, fool me once shame on you, fool me twice shame on me. And I want to know what we can learn from this. Now this is not the first time that a data breach has happened. Perhaps it is the biggest that has ever happened, but it has happened to other companies before.

Now to the extent that you weren't prepared for this or that it happened to you and I hope that was not due to complacency, I hope it was not due to you not doing everything that you could to have prevented it, but my question is this. Can you share with us any information about the attackers? What do you know and what do you not know about them at this point?

Mr. SMITH. Congressman, thank you for that. As I mentioned in my opening comments and my written testimony, earlier this week we have engaged the FBI and they currently have the investigation in their hands. So at this juncture we are not disclosing what we know about the hackers.

Mr. CARTER. How has your cooperation with the FBI been? Has your experience with them thus far been good and anything that—this is important. It is important for everyone. Yes, everyone is upset and rightfully so. They should be upset. When your personal data is out there obviously it is very upsetting. But I am trying to go in a different direction. I am trying to figure out how we can prevent this from happening.

Mr. SMITH. The cooperation with the FBI as best I know has been good. It is ongoing. We have lines of communication into the FBI not just after a breach but routinely throughout the year. So I would say it has been a very good cooperation, Congressman.

Mr. CARTER. Let me ask you this. Through this experience, if you had to do anything different what would you have done?

Mr. SMITH. Congressman, I was asked that question earlier and my answer will be the same now as it was earlier. There will be time for reflection personally and as an organization. That coupled with the investigation that we continue to undertake to look at processes in-house. But this juncture, since I was notified in mid-August through this morning, it has all been about the forensics. It has been about trying to protect and do what is right for the consumer and there has been no time to reflect on what I would do differently.

Mr. CARTER. OK. Well, when that time comes we need to know, because we don't need to let this happen again and other companies need to learn from it. This is obviously as I said earlier you are not the first company to suffer from this. You are not the first Georgia company to suffer from this. We understand that. It doesn't make it any less egregious to what has happened, but where I am trying to go is what can we do better to prevent this from happening again? These guys are good, we know that. Listen, cybersecurity is hard. It is way above my pay grade, I can tell you that.

Mr. SMITH. Congressman, thank you for that. As I mentioned in my comments I take full responsibility as CEO.

Mr. CARTER. And I understand that and I appreciate that.

Mr. SMITH. If there is one thing I would love to see this country think about is, the concept of a social security number in this environment being private and secure, I think it is time as a country to think beyond that. What is a better way to identify consumers in our country in a very secure way, and I think that way is something different than an SSN, a date of birth, and a name.

Mr. CARTER. Well, you are exactly right. I remember my time in the Georgia State Legislature when we changed the, you used to have your social security number on your driver's license. That used to be your driver's license number, and that was not that long ago. And that is what tells me that this is something that is changing dramatically and quickly and we need to be prepared for it.

So I know that you are putting out fires right now, but at some point we need to learn from this. We need to know, look, we shouldn't have done this and we should have done that. What could we have done differently? What will benefit another company to allow that this doesn't happen? And I hope, and thus far you appear to have been honest about all this, I hope that if part of what the problem was complacency that you admit that and say don't ever let your guard down.

Mr. SMITH. Thank you, Congressman. I would love to be part of that dialogue about what lies ahead to protect individuals' identities.

Mr. CARTER. Well, again I want to thank you for being here and it says a lot about you and about your company.

Thank you, Mr. Chairman. I yield back.

Mr. LATTA. The gentleman yields back. The chair now recognizes the gentlelady from California for 5 minutes.

Ms. ESHOO. Thank you, Mr. Chairman. First, I would like to recognize a former colleague that is here in the chamber with us.

Saxby Chambliss who served in the House and in the Senate, it is good to see you, very nice to see you.

Mr. Smith, it seems to me that you have accomplished something that no one else has been able to accomplish and that is that you have brought Republicans and Democrats together in outrage and distress and frustration over what has happened, because this is huge. This is almost half of the country and their information.

The American people are, I think they have privacy in their DNA. We don't like Big Brother. We don't like people having information on us. We know in an information age and then the digital age that that is impossible, but boy, when that is breached, when the privacy goes out the window it really puts a dent in people's lives. I equate it with because they don't feel that they can do anything about it. They feel helpless. I come from earthquake country and when that rattle first starts you really do feel helpless. You feel absolutely helpless.

Now, the question has been posed rhetorically by some members, because I have been sitting in for awhile at this hearing, what can be done. I have the privilege of representing most of Silicon Valley. I have asked this question about the protection in terms of privacy breaches in our country to just about every CEO I have met and they have responded like a chorus and said there are two main reasons for breaches in our country, number one, a lack of hygiene in systems and very poor security management. That is why I have legislation. Senator Hatch is the lead sponsor in the Senate. I have the bill in the House.

So it is distressing to me knowing this information that Homeland Security notified Equifax, this is almost 7 months ago, this has to do with a patch. So I know there are a lot of questions that have probed this, but you as CEO at the time, when Homeland Security informed your company that there was a breach what did you say to your CIO officer? Did you understand what the breach was? Did you understand what the patch meant? Did you understand the timeliness, the need for timeliness to have this fixed and did anything change in that department? Was there a new policy put in place by you?

Mr. SMITH. Congresswoman, to clarify, when the CERT came out in March there was no notification of a breach. There was notification—

Ms. ESHOO. What did it mean?

Mr. SMITH. What it meant was—

Ms. ESHOO. I mean if I got a notice from Homeland Security that is like the FBI knocking on the door. It is the federal government. That in and of itself is a bit menacing, isn't it?

Mr. SMITH. What it meant was an open source software commonly used and deployed around the world called Apache Struts had a vulnerability and the notification was the vulnerability should be patched.

Ms. ESHOO. All right. And did you ask if it was patched?

Mr. SMITH. We get notifications—

Ms. ESHOO. No, you got the notification from Homeland Security, all right? What did you do about it the day you found out? The company was notified on, I believe, the 9th of March. When did you know?

Mr. SMITH. The team, security team followed a protocol and instantly within a day sent notification out to many people in the organization that a patch needed to be applied to Apache Struts.

Ms. ESHOO. And did you ask your team when it was applied?

Mr. SMITH. The security team did and they spoke with the IT team as well.

Ms. ESHOO. When did they take care of it?

Mr. SMITH. Throughout the testimony we talked about what occurred was there was a communicate——

Ms. ESHOO. Well, just tell me when it happened. When was it actually——

Mr. SMITH. The following day communication was sent out to those that needed to be notified.

Ms. ESHOO. You already said that. I want to know when they did it, when they took care of it.

Mr. SMITH. They took care of it in July because we never found it. It wasn't until, if you recall, we had the human error, we did the scan, the technology never found it. In July we saw suspicious activity, took the portal down, found the vulnerability, applied the patch.

Ms. ESHOO. Well, I thank the chairman. We have in the rules of the full committee which are approved at the beginning of every Congress that members of the full committee can participate in subcommittees where they are not members and I appreciate the legislative courtesy. And I think there is a lot more to be done on this issue, Mr. Chairman, if I might make the recommendation. I think we should have the CIO, the chief information officer, come in because I don't think that this resolved. So thank you.

Nice to see you, Saxby.

Mr. LATTA. Thank you very much. The gentlelady's time has expired. And we are just going to ask one quick follow-up question so I am going to yield to the ranking member first.

Ms. SCHAKOWSKY. First of all, Mr. Chairman, I would like to insert for the record a letter from consumer groups, too, a letter from Credit Union National Association, and an article from WGN-TV.

Mr. LATTA. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Ms. SCHAKOWSKY. Oh, sorry.

So in closing, Mr. Smith, I want to quote again from you, from your testimony. You mentioned the five fixes, so-called, and you put, "This puts the control of consumers' credit information where it belongs, with the consumer." So I want to ask you a question. What if I want to opt out of Equifax? I don't want you to have my information anymore. I want to be in control of my information. I never opted in. I never said it was OK to have all my information and now I want out. I want to lock out Equifax. Can I do that?

Mr. SMITH. Congresswoman, that requires a much broader discussion around the rule that credit reporting agencies—because that data as you know, today, doesn't come from the consumer it comes from the furnishers and the furnishers provide that data to the entire industry.

Ms. SCHAKOWSKY. No, I understand that and that is exactly where we need to go, to a much larger discussion because most Americans really don't know how much information, what it is,

that you have it, and they never said OK. So I am hoping this will lead to a wider discussion. Thank you.

Mr. LATTA. Thank you very much. The gentlelady yields back. And if I may just go back to what we had a little discussion earlier, again going back to your testimony. From August the 15th when you were informed that it appeared likely that consumer, that information had been stolen, again why was there again a 10-day delay between finding out about that personal information that could have likely been stolen to developing that remediation plan? That 10-day window, why did it take 10 days to start that remediation?

Mr. SMITH. Well, Congressman, there was continuous motion going on around the clock from that time through yesterday trying to develop the product, build the communication plan, stand up web sites, inform those that needed to be informed. It wasn't like on a certain date something occurred, it was continual motion by many people for many, many weeks.

Mr. LATTA. Let me ask just a quick follow-up on that then, because again with that 10-day period of time, when was the appropriate time that it was really to start talking to the consumers at that point in time or again waiting until when you did in September? Because again there was that lag time there when information could have been stolen on individuals.

Mr. SMITH. Yes. The whole goal was to make sure the data we had was accurate, was as clear for the U.S. consumer as possible. Number two was to make sure for the forensic cybersecurity specialists that our environment was as secure as possible. Remember, they said expect increased attacks. Number three was to stand up the call centers and the web sites for hundreds of millions of consumers and that just took time as I alluded to earlier.

Mr. LATTA. Well, thank you very much. And seeing that there are no other members present to ask questions, we want to thank you very much for testifying before the subcommittee today. And pursuant to committee rules I remind members that they have 10 business days to submit additional questions for the record and I ask that the witness submit his response within 10 business days upon request of any questions submitted. Without objection, the subcommittee is adjourned.

[Whereupon, at 1:03 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

#### PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

Today the DCCP subcommittee will focus on a massive data breach executed against Equifax, but this is just one of many recent data breaches nationwide. Millions of consumer data, including personally identifiable information, have been compromised leaving customers vulnerable to criminal entities operating mostly on the dark web. In addition, Equifax did not notify consumers until 40 days after observing suspicious traffic and shutting down the source of this traffic.

In an effort to quickly respond to consumers, Equifax's website and call centers were overwhelmed and initially unable to inform individuals if their information had been compromised. Another frustrating factor was the inclusion of a mandatory arbitration clause in the terms and conditions of credit monitoring services being offered, but I understand this has since been removed.

The issue of data breach notification has been before this subcommittee for many years. There is a history of bipartisan cooperation, indicating a strong desire to get this right for all consumers. At this point, there is likely not a single Member of

Congress who has not had a constituent, or themselves, affected by a data breach or cyber attack. Without a reasonable federal standard on data security and breach notification, companies are implementing various security protocols and hoping they don't become the next victim of a breach. The lack of a single, federal standard has led to numerous state laws, but data breaches transcend physical boundaries.

Last Congress, this subcommittee passed the Data Security and Breach Notification Act, which would have required breach notification to customers within 30 days, including ways to inquire with the company as well as how to contact the Federal Trade Commission. Companies also had to alert customers that reasonable measures were taken to restore the integrity, security and confidentiality of the data system.

One of the most important sections of the bill would have required entities to implement and maintain reasonable security measures and practices appropriate to the size and type of entity, as well as protect personal information against unauthorized access. These reasonable measures are based on industry accepted practices while remaining flexible to allow advancement in accordance with the security technology market. Currently, such measures might include 2-factor authentication as well as immediate patching of known software vulnerabilities. According to Mr. Smith's testimony, the flaw used to perpetrate the Equifax breach was a known security vulnerability that had an existing patch.

Had the Data Security and Breach Notification bill passed out of this committee with bipartisan support, it may well have become law and prevented, or at least softened the blow of, a data breach on the massive scale experienced by Equifax.

As we work through what happened and how consumers can recover their data security, I hope we can again find bipartisan consensus on data security and breach notification going forward.

---



3 October 2017

**RE: Equifax Breach Response**

Dear Member of the Committee on Energy and Commerce,

We, the undersigned consumer, community and other organizations write in advance of this week's House and Senate hearings into the massive and unprecedented breach of personal information held by Equifax, including Social Security Numbers and dates of birth for 143 million consumers. We write to express our grave concerns over the company's slow response to the breach and then its shifting, maddening, and ultimately inadequate response to consumers including our members, clients and other constituencies. We write with several recommendations for what Congress should and should not do in response.

**First, the Equifax scandal underscores the importance of the Consumer Financial Protection Bureau's rule to protect a citizen's right to sue financial companies.** While Equifax *appears* to have finally dropped the applicability of its forced arbitration clauses for consumers taking advantage of any parts of its relief package, the company continues to include clauses in its fine print in other places that forbids a consumer from taking the company to court (see <http://www.equifax.com/terms/>). Further, this unjust limitation of consumer rights would still apply to other consumers of Equifax products. Its actions, and those of Wells Fargo, show the need for all consumers of all financial firms to have their day in court restored to make the marketplace work more fairly.

**Second, Congress should enact free credit freeze legislation immediately.** Consumers are not credit bureau customers, we are their product. The only way for us to secure our credit reports from being accessed by an identity thief applying for new credit in our names is to "freeze" our credit, then lift or "thaw" it temporarily whenever we plan to apply for credit. Yet, except in a few states, nearly all consumers, with a few exceptions for seniors and others, must pay a fee of up to \$10 each time they freeze or thaw their own credit reports. While Equifax says that it will soon offer a similar "lock" product for free, consumers deserve to have a right to this control by law, and without cost. Furthermore, it must apply to all of the so-called "Big 3" credit bureaus, Equifax, Experian and TransUnion, because protecting your credit report at only one leaves two doors open.

**Third, Congress should resist attempts from the financial and other industries to pass weak federal breach notice legislation that preempts stronger state laws.** Every time there is a major data breach, industry actors urge passage of federal legislation that limits when consumers are required to be notified, defines harms narrowly, and limits consumer and state legal rights. Furthermore, these industry actors seek bills that would broadly preempt any state activities, not just on breach notification, but data security and privacy as well. While we are very troubled that Equifax delayed notification, possibly in violation of state breach notification laws, we are confident that

an ongoing bi-partisan state attorneys general investigation will hold the firm accountable for that.

**Fourth, Congress should consider the need to reform all the activities of the Big 3 credit bureaus, as well as specialized consumer reporting agencies.** Consumer reporting agencies, including the Big 3 credit bureaus and other specialized agencies are regulated by the 1970 Fair Credit Reporting Act (FCRA). "Larger participant" consumer reporting agencies, including the Big 3, are under the supervisory and examination authority of the Consumer Financial Protection Bureau for their credit reporting businesses. The CFPB has begun in just a few years to rein in the worst practices of the Big 3 credit bureaus, such as deceptive marketing of subscription credit monitoring products and failure to comply with existing law's requirements on conducting reasonable dispute reinvestigations. This is important, as the Big 3, in particular, are powerful gatekeepers to financial and employment opportunity, yet numerous studies have shown that their deficient procedures and industry favoring practices result in too many mistakes that harm consumers.

But Congress should also understand that the bits and pieces of our financial DNA lost by Equifax remain under the jurisdiction of the Federal Trade Commission (see Dodd-Frank Section 1093, which excludes CFPB from the Gramm-Leach-Bliley Act's data security provisions). FTC has limited to no authority to write regulations, conduct supervisory examinations, investigate violations, or impose penalties.

In closing, we urge Congress to take firm and assertive actions to ensure consumers are not further harmed, but made whole, after this egregious data breach by Equifax. If you or your staff have any questions, please contact Ed Mierzewski of U.S. PIRG at [202-461-3821](tel:202-461-3821) ([edm@pirg.org](mailto:edm@pirg.org)) or Chi Chi Wu of the National Consumer Law Center at [617-542-8010](tel:617-542-8010) ([cwu@nclc.org](mailto:cwu@nclc.org)).

Thank you for your consideration,

Americans for Financial Reform

Allied Progress  
Center for Digital Democracy  
Consumer Action  
Consumer Federation of America  
Consumer Watchdog  
National Association of Consumer Advocates  
National Consumer Law Center (on behalf of its low-income clients)  
Public Citizen  
Tennessee Citizen Action  
U.S. PIRG  
Woodstock Institute



Jim Nussle  
President & CEO

Phone: 202-508-6745  
jnussle@cuna.coop

601 Pennsylvania Avenue NW  
South Building, Suite 600  
Washington, D.C. 20004-2601

October 3, 2017

The Honorable Bob Latta  
Chairman  
House Energy and Commerce Subcommittee  
on Digital Commerce and Consumer Protection  
Washington, DC 20515

The Honorable Jan Schakowsky  
Ranking Member  
House Energy and Commerce Subcommittee  
on Digital Commerce and Consumer Protection  
Washington, DC 20515

Dear Chairman Latta and Ranking Member Schakowsky:

On behalf of America's credit unions, thank you for holding the hearing titled, "Oversight of the Equifax Data Breach: Answers for Consumers." The Credit Union National Association (CUNA) represents America's credit unions and their 110 million members.

The massive Equifax data breach has put more than 143 million American consumers at risk by exposing consumers' most personal information along with hundreds of thousands of credit card numbers. Stolen information includes personally identifiable information (PII), including Social Security numbers, birth dates, and driver's license numbers and payment card data including credit and debit card numbers.

CUNA has voiced its intent to file a lawsuit to protect credit unions and their members from harm resulting from the Equifax data breach. The breach has harmed and will harm credit unions and their members. Hackers had access to highly sensitive PII and payment card data for months exposing credit unions to damages in replacing members' payment cards, covering fraudulent purchases and taking protective measures to reduce risk of identity theft and loan fraud and assuming financial responsibility for various types of fraudulent activity related to stolen identities and misuse of PII and payment card data.

Equifax and the other two credit reporting agencies (CRAs) are integral to the loan underwriting process facilitating the extension of credit by credit unions, banks and others to American consumers. Credit unions, banks and others provide Equifax with their members' and customers' information so that Equifax may use its expertise to aggregate, process and analyze information so that it can be marketed to the financial services industry and to consumers directly. Credit unions and banks also purchase information from Equifax and other CRAs for the purposes of analyzing credit worthiness and financial condition of consumers and provide purchase information to Equifax and the other CRAs.

We encourage you and your colleagues to ensure that consumers impacted have been properly notified and that Equifax has taken all measures to ensure that consumers are not at further risk. On behalf of America's credit unions, thank you for holding today's hearing. We look forward to continuing to work with you on this important issue.

Sincerely,

Jim Nussle  
President & CEO

<http://wgntv.com/2017/10/01/equifax-investigating-stock-sales-made-by-executives-during-data-breach/?shared=email&msg=fail>

Equifax investigating stock sales made by executives during data breach

POSTED 5:15 PM, OCTOBER 1, 2017, BY CNN WIRE

Americans are outraged about the Equifax data breach that exposed the personal and financial data of 143 million people.

Equifax is investigating three executives who sold company shares worth nearly \$2 million shortly after a massive data breach was discovered, but before the company announced the breach to the public.

The investigation was disclosed in a letter Friday to Rep. Frank Pallone, the lead Democrat on a House committee looking into the Equifax data breach.

"Equifax takes these matters seriously," said Equifax said in response to a letter from Pallone that raised questions about the stock sale.

"The board of directors has formed a special committee. The committee has retained [outside] counsel and is conducting a thorough review of the trading at issue."

The company did not respond to a request for comment about the probe.

Equifax has confirmed that it found out about the hack on July 29, although it said it took some time to learn just how much information was exposed. It says that at least 143 million Americans had sensitive

<http://wgntv.com/2017/10/01/equifax-investigating-stock-sales-made-by-executives-during-data-breach/?shared=email&msg=fail>

financial data compromised, including social security numbers. CEO Richard F. Smith left the company Tuesday in the wake of the hack.

According to filings with the SEC, Equifax Chief Financial Officer John Gamble sold shares worth nearly \$950,000 on August 1. Joseph Loughran, Equifax's president for U.S. information solutions, sold shares on the open market worth about \$584,000 on August 1 as well. And Rodolfo Ploder, president of workforce solutions, sold stock for more than \$250,000 on August 2.

Those shares were sold at prices of \$145.00 or more. But Equifax shares plunged to \$121.82 at the start of trading the first day after the hack was announced. That means the three executives netted an additional \$300,000 between them by selling before the disclosure was made.

After the hack was disclosed, Equifax told CNNMoney that the sales of stock represented a "small percentage" of the shares owned by the three executives, and that they all "had no knowledge that an intrusion had occurred when they made the sales."

Earlier this month 37 U.S. senators wrote to Justice and the Securities and Exchange Commission last week asking that the stock sales be examined by those enforcement agencies.

The retirements of both Chief Security Officer Susan Mauldin and Chief Information Officer Dave Webb were announced earlier this month.

GREG WALDEN, OREGON  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641

October 19, 2017

Mr. Richard F. Smith  
Former Chairman and CEO  
Equifax Inc.  
1550 Peachtree Street, N.W.  
Atlanta, GA 30309

Dear Mr. Smith,

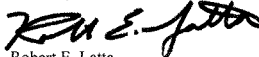
Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on Tuesday, October 3, 2017, to testify at the hearing entitled "Oversight of Equifax Data Breach: Answers for Consumers."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Thursday, November 2, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [ali.fulling@mail.house.gov](mailto:ali.fulling@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Robert E. Latta  
Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection  
Attachment

Additional Questions for the RecordThe Honorable Robert E. Latta

1. In your testimony, you stated “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.”
  - a. What is the name of this cybersecurity firm?
  - b. When was this firm engaged by Equifax to provide this security assessment?
  - c. What is the specific scope of work relating to the assessment of the company’s information security systems that Equifax requested to be completed by the firm?
  - d. Why did Equifax engage this firm if Mandiant was already under contract with Equifax?
2. According to a Bloomberg Businessweek investigation, allegedly “Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, a person familiar with the perspectives of both sides said.”<sup>1</sup>
  - a. Did Mandiant, in fact, convey these warnings to Equifax management, and did company officials agree with the Mandiant assessment?
  - b. When did Mandiant first issue to you or Equifax senior management warnings that unpatched systems could indicate major data breach and data theft problems?
  - c. Please detail each time in 2017 that Mandiant issued such warnings to you or the company.
  - d. If Equifax disagreed with Mandiant on the security assessment or for any other reason, did any disagreement materially affect the time to address the breach and to initiate the breach notification and consumer protection remediation?
  - e. What impact did any disagreement with Mandiant have on engaging the new, well-known cybersecurity firm you noted in your written testimony?
3. According to a Bloomberg Businessweek investigation, reportedly “there [were] signs that Smith and others were aware something far more serious was going on. The investigation in March was described internally as ‘a top-secret project’ and one that Smith was overseeing personally.”<sup>2</sup> According to your testimony, the early March timeframe was when the U.S. Computer Emergency Readiness Team dispatched its notice on the Apache Struts vulnerability.
  - a. Please describe this “top-secret project” or any other direct discussions you were a part of regarding Equifax’s cybersecurity practices or vulnerabilities from January 2017 to July 29, 2017.

<sup>1</sup> <https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros>

<sup>2</sup> Id.

4. In your testimony you noted “the breach occurred because of both human error and technology failures. These mistakes – made in the same chain of security systems designed with redundancies.”
  - a. What was the specific process for reporting cybersecurity vulnerability issues and data breaches up to the CEO’s office, other senior executives, and the board of directors from January 2017 to July 29, 2017?
  - b. What was the specific process for reporting cybersecurity vulnerability issues and data breaches up to the CEO’s office, other senior executives, and the board of directors after July 29, 2017?
  - c. How many reports about unauthorized access into Equifax’s system did you receive as CEO?
  - d. What was the standard used by your direct reports to determine when an event qualified to tell you about the unauthorized access?
5. Please describe the resources, investments and operating expenditures that Equifax had focused on its information security prior to July 2017 for the three preceding years?
  - a. What percentage of Equifax’s balance sheet for the last three years was put into maintaining and upgrading the company’s global IT security systems?
6. Prior to the breach, who did the former Chief Security Officer at Equifax report to? How many full-time employees were employed in the Information Security office?
  - a. After the breach, who does the Chief Security Officer at Equifax report to? How many full-time employees are now employed in the Information Security office?
7. Prior to the breach, who did the former Chief Information Officer at Equifax report to? How many full-time employees were employed in the Information Technology office?
  - a. After the breach, who does the Chief Information Officer at Equifax report to? How many full-time employees are now employed in the Information Technology office?
8. What percentage of Equifax’s balance sheet for the last three years was put into hiring, training and retention of security and/or information technology (application owner) employees? What is the percentage following the breach?
9. In your testimony you mentioned “suspicious activity” numerous times, and seemed to distinguish “suspicious activity” with a breach incident. Is there a meaningful difference between suspicious activity and a breach in how events are reported up the security and information technology departments at Equifax during your tenure? Please describe the differences and if any different terminology was used internally to describe events were unauthorized actors gained access to the Equifax system and/or removed data (personal or otherwise) from the Equifax system.



10. How many individuals have successfully completed the process to enroll in the free remediation product offered by Equifax after the breach? How many individuals have completed the initial sign up step to enroll in the product but have not completed the enrollment process? Please explain in detail any difference between these two numbers and what is being done to address any backlogs.

**The Honorable Brett Guthrie**

1. Thank you for testifying before our Subcommittee. My question relates to concerns I've received from constituents attempting to sign up for the credit freeze or free credit monitoring features through your website and phone hotline.

The primary concern is that when consumers attempt to sign up online they are having trouble navigating to the form page required to file their requests. Some consumers are nervous about submitting their information online, but they are also finding it difficult to navigate the telephone menu options, sometimes even finding the choices circuitous.

- a. Are you aware of these issues that my constituents have raised regarding the challenges of the telephone and online processes?
- b. What specific steps are you taking to simplify the online forms and telephone hotline to make a more direct connection to the required forms and call center professionals, ensuring that consumers are able to take advantage of the services you are offering?

**The Honorable David B. McKinley**

1. So far, 730,000 West Virginians were affected by the breach. That's nearly 40 percent of our population. With so many people affected, communication with law enforcement and other bodies is important, from the federal level all the way down to the local level.
  - a. When did Equifax alert federal law enforcement and other authorities to the data breach?
  - b. Can you please specify what Federal and regulatory authorities were alerted, when, and what action each organization suggested or required?
  - c. At what point did the company alert State law enforcement and other authorities to the data breach?
  - d. Did Equifax inform any of its State regulators of the breach before informing the public?
2. Why weren't the states notified earlier so they could better prepare a plan to inform their residents and set up additional resources for concerned consumers?
3. How have you assisted state and local bodies in their efforts to inform their residents?
4. Do you think you could be doing more to inform potentially affected consumers?

**The Honorable Markwayne Mullin**

1. At least 1.7 million Oklahomans are impacted by this serious breach. I hope they do not experience any incidents of fraud or identity theft as a result, but I imagine some may. Did Equifax have a breach response plan in place before the event that outlined steps the company should take to protect consumers in the event of a data breach?
2. If there was a response plan, did it include immediately notifying customers if their private information was revealed? What other protections or actions are captured in the breach plan?
3. I had several constituents contact my office very frustrated after having spent hours on the phone unable to connect with Equifax customer service. Why were consumers unable to reach anyone by phone?
4. In your written testimony you reference two of your call centers in Florida being taken offline due to Hurricane Irma. Did you alert Experian or TransUnion? Couldn't they have taken some of the load if consumers wanted to activate an initial fraud alerts?
5. How many consumers have signed up for Equifax credit freeze services since September 7, 2017?
6. Will Equifax be refunding fees or charges to potentially impacted customers who enrolled to freeze their credit reports after the breach but prior to September 7, 2017?

**The Honorable Jan Schakowsky**

1. In your written testimony, you stated that Equifax will offer a new free credit lock product that "has been under development for months" and will be available by January 31, 2018. The free TrustedID Premier package currently offered to consumers in the wake of the breach already includes a credit lock tool. And I understand that outside of the TrustedID Premier package, Equifax had been offering a monthly subscription service for locking and unlocking.
  - a. We have been told that this free credit lock tool that will be available by January 31, 2018, could require consumers to consent to Equifax sharing or selling the information it collects from the service to third parties. What third parties will Equifax share or sell information collected about consumers from their use of this new credit lock tool?
  - b. Equifax is not currently offering any new subscription products. But for the credit lock product that Equifax had been offering as a subscription product, how much did that service cost per month? How many locks and unlocks were permitted per month in that program? What was the total cap on locks and unlocks under the program?
  - c. Why has it taken months to develop the new credit lock tool that will be offered by January 31, 2018, when you already have credit locking tools available?
    - i. In addition to the cost, please detail with specificity the differences between the new free credit lock tool that Equifax will begin offering in January and the credit lock tool that had been offered as a subscription service. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.

- ii. You testified at the hearing that the credit report lock that is part of TrustedID Premier is only web-enabled and that the credit lock tool that will be available by January 31, 2018, will be an application. Please explain that comment in more detail. In addition to that difference, please detail with specificity all other differences between the credit report lock that is part of TrustedID Premier and the credit lock tool that will be available by January 31, 2018.
- d. How does a credit lock differ from a credit freeze?
  - i. Please detail with specificity the differences between the credit lock tool that Equifax had been offering as a subscription service and a credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.
  - ii. Please detail with specificity the differences between the credit lock tool that is part of TrustedID Premier and a credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.
  - iii. Please detail with specificity the differences between the new free credit lock tool that Equifax will begin offering in January and a credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.
  - iv. In the FAQs on [equifaxsecurity2017.com](http://equifaxsecurity2017.com), Equifax states:
    - Security freezes were created in the early 2000's, are subject to regulation by each state and use a PIN based system for authentication.
    - Credit file locks were created more recently, are mobile-enabled and use modern authentication techniques, such as username and passwords and one-time passcodes for better user experience.
- A. For Equifax's credit lock tool that will be available by January 31, 2018, please specify the provisions of each state regulation that the credit lock tool will not have to comply with but that credit freezes do have to comply with.
  - B. Please explain in detail why a username and password is a better experience than a PIN-based system for users. Please explain how usernames and passwords are more secure than PINs.

- e. Yes or no: will the credit lock tool that will be available by January 31, 2018, require consumers to agree to a mandatory arbitration clause to use the tool? Please provide a copy of the anticipated terms of service for this tool or detail with specificity the terms of service that Equifax expects will be associated with this tool.
  - f. Consumer Reports has said, "In most cases a credit freeze offers better protections against fraud, making it the best option." Do you agree with Consumer Reports? What rights and recourse does a consumer have if the lock system fails? What rights and recourse does a consumer have if a credit freeze fails? Please specify by state as necessary.
  - g. How specifically does a credit lock help prevent the consequences of identity theft that are not related to opening new lines of credit, such as fraudulent tax refunds, fraudulent insurance claims, and the many other types of fraud that may occur?
  - h. Consumers can still choose to freeze their credit instead of using a credit lock tool. For those consumers, other than those living in states with fee limitations, how much does it cost to freeze their credit? How much does it cost to unfreeze their credit?
2. Equifax is offering consumers one free year of a package of services called TrustedID Premier. It includes credit monitoring at the big three CRAs, copies of your Equifax credit report, identity theft insurance, Internet scanning for your Social Security number, and the ability to lock and unlock your Equifax credit report.
- a. Yes or no: do you expect all attempts at identity theft to occur within one year of this breach?
  - b. Why isn't Equifax offering TrustedID Premier for longer than a year?
  - c. Within the year that consumers may have the TrustedID Premier service, how specifically does that package of services help prevent the consequences of identity theft that are not related to opening new lines of credit, such as fraudulent tax refunds, fraudulent insurance claims, and the many other types of fraud that may occur?
  - d. How will Equifax compensate victims for each of the potential consequences of identity theft? Has Equifax set aside funds to compensate victims for things like insurance and legal costs? If so, how much has been allocated? If not, do you plan to do so?
3. Please provide a copy of or describe with specificity the security incident response plan or protocol that Equifax had in place at the time the breach was discovered at the end of July 2017. Was that plan or protocol followed exactly? If not, please specify each step of the protocol that was not complied with and what actions or inactions occurred instead.
4. Please provide a copy of or describe with specificity the breach response protocol and/or crisis management protocol that Equifax had in place at the time the breach was discovered at the end of July 2017. Was that protocol followed exactly? If not, please specify each step of the protocol that was not complied with and what actions or inactions occurred instead.

5. Under the security incident response plan or protocol, the breach response protocol and/or crisis management protocol, or any other protocol in place at Equifax at the time the breach was discovered at the end of July 2017, at what point was the Chief Financial Officer to be notified of a breach? Under such protocols, were outside counsel and outside security firms to be hired before the CFO was notified? Is that standard industry practice?
6. In the wake of this most recent breach, customers were directed to an Equifax customer support website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com). Security researchers have been critical of the website. Some browser security tools blocked the site because it looked fraudulent. It had improper TLS security certificates—an online technology used to transport critical data like Social Security Numbers, which the site was collecting. Further, the domain name was not even registered to Equifax. Consumers have reported that the website keeps crashing or loads slowly.
  - a. You testified at the hearing that Equifax is not providing most breach victims with any notice of the breach other than this website. This site is the only way for consumers to find out if their data was stolen. It is also the only place they can sign up for the free identity theft protection. Why is it still unreliable more than a month after the breach was made public?
  - b. Why was it not a higher priority at Equifax to ensure your consumer response website worked well and was secure? If Equifax was too overwhelmed in to do so internally, why didn't you hire an outside firm to build a secure site for consumers?
  - c. When a consumer attempts to sign up for TrustedID Premier, and chooses to answer the many questions required, the consumer is told after submitting the online forms that he or she will receive an email with a link to finalize and activate the product and that there may be a delay before receiving that email. There is no immediate confirmation email that the consumer's interaction with Equifax was even successful so the consumer does not know when or if she will hear back. When should a consumer assume the first interaction was not successful and try again? Why did you decide against having a confirmation email sent to the consumer?
  - d. Why did Equifax set up a new website that is completely separate from the Equifax.com for the consumer response to the breach? Did you consider having the consumer response information on your main homepage at Equifax.com? If the main site could not handle the consumer volume, why not just improve your original site if it was insufficient?
7. Equifax's Twitter account had directed consumers to a fake version of the consumer response website multiple times.
  - a. Who is responsible for Equifax's Twitter page? What information or training was provided to that person or persons with regard to the breach and Equifax's response to the breach?
  - b. What steps has Equifax taken to ensure such misinformation will not happen again?

8. Equifax has now reported that the personal information of approximately 145.5 million Americans was affected by this breach. You explained in your testimony that access to that personal information occurred through Equifax's online dispute portal. But most of people whose information was stolen had never used the online dispute portal at any time in the existence of the portal nor had most of them ever filed a dispute with Equifax through another means. Please explain in detail how the hackers were able to access and acquire the information of 145.5 million Americans by gaining access through the consumer-facing online dispute portal.
  - a. Where was the accessed information stored? Was all the information available to the dispute portal or were the hackers able to move through Equifax's systems?
  - b. What specific datasets or systems were access by the hackers using the dispute portal?
  - c. According to equifaxsecurity2017.com, "criminals also accessed credit card numbers for approximately 209,000 U.S. and Canadian consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers." Are those additional consumers included in the current 145.5 million number?
9. Limiting access to credit even for a short period of time can have real financial consequences, especially for low-income populations. How quickly will a credit file be able to be locked and unlocked with the feature expected in January and how will you ensure that speed? For example, Equifax was not able to handle the calls coming in from this breach. How can we be sure it will be able to lock and unlock quickly for the entire population of consumers?
10. Please confirm that under the credit lock tool that will be available by January 31, 2018, consumers will be able to unlock or lock only their Equifax credit file for free for an unlimited number of times per month for their lifetimes. Please confirm that consumers will be able to sign up for this free service at any time in the future.
11. Equifax is only one consumer reporting agency (CRA) out of dozens and one of four major CRAs.
  - a. Do you agree that locking or freezing at only one agency will leave consumers at risk?
  - b. Yes or no: will Equifax pay for free credit freezes at the other CRAs or reimburse victims for the money they have to spend to freeze or lock their credit at other CRAs? Yes or no: will Equifax pay for victims to temporarily lift credit freezes as needed?
  - c. Do you support a quick one-stop freeze and unfreeze concept so that consumers can freeze their credit at all agencies at once?
12. Equifax was hit this time, but all consumer reporting agencies are targeted by cybercriminals because of the vast amount of valuable personal information they possess. Since this is an industry-wide threat, do Equifax and other CRAs share threat information with each other or work together to prevent cyber threats?
13. Credit report accuracy has historically been a big problem for CRAs, and consumers have often had trouble getting CRAs to correct mistakes in their reports.
  - a. What is Equifax doing to ensure it can respond promptly and accurately if more credit reports need to be corrected as a result of this breach?

- b. If victims of this breach do have fraudulent items on their credit report, what is Equifax doing so that the victims can feel secure submitting documents to your dispute resolution website if they have to?
- 14. Equifax notified the Federal Bureau of Investigation on August 2, 2017, that a cyberattack on a portal containing consumer information had occurred. The Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) were not notified until September 7, 2017, the same day Equifax made the public announcement of the breach. You testified already that you were informed by August 15, 2017, that personally identifiable information was likely stolen. Why did Equifax not notify the FTC or CFPB earlier?
- 15. You wrote in your testimony that you “are ultimately responsible for what happened on [your] watch” at Equifax. Yet the term being used to describe your exit last week after 12 years with the company is “retired”—not resigned or fired. Equifax’s board has reportedly retained the right to retroactively classify your departure as “being fired for cause.”
  - a. What conditions would lead the board to redefine your exit as “being fired for cause” rather than “retiring”?
  - b. Is there a deadline after which the classification of your exit from Equifax cannot be altered?
  - c. Was your testimony on at the hearing on October 3, 2017, a condition for your ability to “retire” and retain your compensation package?
  - d. Roughly how much of your compensation would you retain even if you were retroactively fired for cause?
- 16. You wrote in your testimony that the board was involved in the development of Equifax’s consumer response after you notified it of the breach in late August.
  - a. Did the board approve the original and insufficient “consumer notification and remediation program” that Equifax rolled out on September 7?
  - b. Did the board approve the multiple-week delay in notifying customers of the breach?
- 17. Equifax needs to reexamine and substantially improve the way it treats consumers. I am concerned that the company has chosen to replace you as Chairman with a board member, Mark Feidler, who was part of Equifax’s botched response—and even served on the board’s Technology and Governance committees during the breach.
  - a. What was Mr. Feidler’s role in developing and implementing Equifax’s consumer response to this breach in August and September?
  - b. You are an unpaid advisor to Equifax right now, and your association with the company ends in less than three months. But the effects of this breach will be felt by consumers long after that. Will the company commit to having its interim CEO, and the new permanent CEO when one is hired, come back to this committee provide further updates if necessary?

18. A patch for the vulnerability that led to the breach was issued on March 8, 2017, and Equifax confirmed that it was aware of the patch at that time and worked to identify and patch vulnerable systems. You testified that the Equifax security department required this vulnerability to be patched within 48 hours, consistent with the Equifax Patch Management Policy. But you testified that the vulnerability was not identified or patched.
- a. Please provide in detail the organizational structure of Equifax at the time of breach, including the entire reporting structure below the Chief Security Officer, the entire reporting structure below the Chief Information Officer, the reporting structure from the Chief Security Officer to the Chief Executive Officer, and the reporting structure from the Chief Information Officer to the Chief Executive Officer.
  - b. It is my understanding that the Chief Security Officer reported to the Chief Legal Officer/General Counsel. Is that common practice in the credit reporting industry? Is that common practice in the data broker industry?
  - c. Who within the company knew or should have known on which applications Apache Struts was running? Who within the company maintained the master list of all applications and what software was running on each application?
  - d. Please describe with specificity Equifax's patch management policy that was in effect in March 2017. What changes have been made to that policy since the breach was discovered in July 2017?
  - e. Please describe with specificity Equifax's process as of March 8, 2017, for applying patches and verifying that a patch had been applied correctly. Please include what person, position, or office is responsible for each step in that process. Specify the role of the application development team (including the reporting structure), the role of the infrastructure team (including the reporting structure), and the role of the security team (including the reporting structure).
  - f. In March 2017, where in the internal chain of command did primary responsibility for correctly installing updates fall? Was there an escalation process if a patch was not applied promptly and correctly?
  - g. The current Chief Security Officer told committee staff that when notified of a vulnerability that required a patch, the application development team would initiate a change ticket for the patch and the infrastructure team would implement the patch. Then a security scan would be run to ensure the patch was applied.
    - i. Yes or no: is this an accurate statement of the patching process? If no, please explain.
    - ii. Who received notifications when a change ticket was not completed?
    - iii. Did the application development team, the infrastructure team, the information technology team, or any team/department other than the security team who reported to the Chief Security Officer have a method of determining that patches were applied? If so, please explain in detail with regard to each team/department/office that had such methods.



- h. The former Chief Security Officer told committee staff that security scans searched for vulnerabilities, not for properly applied patches. She said that an initial scan was run before the patch for the Apache Struts vulnerability was applied and no vulnerabilities were found. The IT team then applied the patches and that team had ways to determine if the patches were applied. Security did not rescan after the patches were applied because no vulnerabilities were found in the initial scan and, therefore, no vulnerabilities would be found after the patches were applied. Yes or no: is this account accurate? If no, please explain.
  - i. Yes or no: was the scan for vulnerabilities the only method of ensuring that patches were applied?
- 19. Mandiant conducted a forensic investigation of what happened in this incident and produced a report, which was finalized on October 2, 2017. Please provide a copy full report.
- 20. Press reports indicate that Mandiant was working for Equifax in March regarding another Equifax breach. That investigation was described internally as "a top-secret project" that you were personally overseeing.
  - a. Why did you oversee that breach personally and not the breach that was the subject of this hearing?
  - b. What changes in security practices, procedures, and protocols were made following that March breach as well as the other three most recent Equifax breaches?
- 21. Press reports also indicate that Equifax's relationship with Mandiant broke down, but Mandiant had warned that unpatched systems indicate major problems.
  - a. What specific information and advice did you receive from Mandiant at that time? Did you personally get the warning? Who else in the company received that warning?
  - b. What steps were taken in response to that warning?
  - c. If you were unhappy with Mandiant in March, why hire it again?
- 22. Equifax reported that unauthorized access to consumer data started on May 13, 2017. One large financial firm told the *Wall Street Journal* that it saw a spike in fraudulent activity using the same types of data stolen in the breach starting in late May.
  - a. Do you know if the criminals have used or sold the data that was stolen? Has Equifax performed any analysis to see if fraud alerts or credit report disputes for your own reports have increased since May?
  - b. Is Equifax aware of a noticeable increase in synthetic identity theft where the fraudster takes data points from multiple established identities in recent months or years?
- 23. I understand Equifax has changed its reporting structure in the wake of the breach. Please provide in detail the current organizational structure of Equifax, including to whom the new Chief Security Officer reports and to whom the Chief Information Officer reports.

24. Susan Maudlin, the former Chief Security Officer told committee staff that she informed John Kelley, the Chief Legal Officer, to whom she regularly reported, of the breach by July 31, 2017. She also said that at the same time Mr. Kelley was informed that the incident may have compromised personally identifiable information.
  - a. Do you and Equifax deny that assertion?
  - b. Is it true that Mr. Kelley is still Chief Legal Officer for Equifax?
25. Your testimony noted a “mounting concern” as of September 1, 2017, that Equifax’s system had to be prepared for new “copycat” and other attacks after public notification of the breach.
  - a. Who informed you of that concern? When were you first informed of that concern? When did Equifax begin preparing its systems for those anticipated attacks? Did Equifax wait until September 1?
  - b. What preparations were made for those attacks? Were those preparations completed before public notice occurred on September 7?
26. When and why did you decide that September 7 would be the day you announced the breach?
  - a. What day were employees at your customer service call centers informed about the breach?
  - b. How were call center employees trained to help consumers and answer questions about the breach?
  - c. Did you hire additional employees for the call centers before September 7? If not, why?
  - d. When did you start building the website? Had you subjected it to any performance tests or security audits before September 7?
27. What could Equifax have done differently to provide consumers with better support and more information earlier? What is Equifax doing now to provide consumers with better support and more information going forward?
28. On August 17, 2017, at least two days after you knew about the breach and that personally identifiable information was compromised, you said in a speech, “[f]raud is a huge opportunity for [Equifax]. It is a massive, growing business for us.” What did you mean by that comment?
29. According to media reports, Equifax has had a number of other problems protecting consumers’ personal information. There have been a number of incidents in which a customer was inadvertently sent or able to view credit information of other customers. One report indicated that a customer was inadvertently sent hundreds of credit reports, which included personal information, of other consumers. What practices does Equifax have in place to detect and respond to such data leaks and inadvertent disclosures of consumers’ personal information?

**The Honorable Ben Ray Lujan**

1. Extensive weaknesses in Equifax's data protection system were revealed after the hacking.
  - a. What, if anything, has been done to address the vulnerabilities on the Equifax website exposed in the data breach?
  - b. Are there now regular audits and other forms of security monitoring currently in place? How often?
  - c. How has the company improved its cybersecurity following the breach?
  - d. What will Equifax do to ensure that consumers affected by the theft of their personal information from your system are made whole?
  - e. What does Equifax do to secure its websites? What changes is Equifax putting in place after this most recent website incident to ensure its websites do not contain malicious links or code?
2. After offering initial resistance to credit freezes, Equifax has made credit freezes or "credit locks" free for one year.
  - a. What specifically are the differences between the one-year credit freeze now offered and the "credit lock" you will be offering?
  - b. There have been a number of recent complaints from customers opting to use Equifax's credit freeze service that they have been unable to temporarily lift their credit freezes online or by phone because of various customer service failures. For example, consumers have reported that the automated phone system provides no means of entering a PIN and that they are unable to reach a customer service agent. Others report website failures prevent them from lifting their freeze online. Could you please provide an explanation? What steps is Equifax taking to ensure that the website is working properly and that customers can easily lift a credit freeze by phone?
  - c. As previously stated, customers could be reeling from the theft of their data resulting from this data breach for years. Why has the company not made credit freezes, in addition to credit locks, free in perpetuity for those affected?
  - d. What is the rationale for offering a free credit freeze for only a limited period of time, when it's clear the stolen data could be used at any time to create fraudulent accounts and otherwise prey on the victims of this breach? Why should consumers in years to come be forced to pay for Equifax's failure to protect their data in the first place?
  - e. During the hearing, you testified that Equifax was not currently working with the other credit reporting agencies to provide protections for consumers impacted by the data breach. Can you provide an explanation as to why your company is not working with Experian and TransUnion to ensure they provide free credit freezes and other reasonable consumer protections? Can you explain why your company is not offering to pay for credit freezes or other reasonable protections on behalf of consumers at Experian and TransUnion?

3. During the hearing, you asserted that from a customer perspective, a credit lock and credit freeze are the same.
  - a. If a credit lock and freeze are the same, why doesn't Equifax simply offer credit freezes, which come with strong, well-understood legal protections for consumers, for free?
  - b. What information about consumers does Equifax collect, share, sell, or otherwise grant access to third parties under a credit lock that it does not under a credit freeze?

**The Honorable John Sarbanes**

1. Can minors have their identity stolen?
2. Does Equifax offer monitoring and security products to protect minors from identity theft?
3. Were any minors impacted by this latest breach? Please explain how you can be sure.
4. Are minors eligible to receive Equifax's free monitoring services? Please explain how this decision was reached and why.

**The Honorable Jerry McNerney**

1. Please provide in detail the organizational structure both prior to and after July 29, 2017 of Equifax's Security Department and its Information Technology Department.
2. What function(s) does the Security Department carry out in the vulnerability patching process?
3. What function(s) does the Information Technology Department carry out in the vulnerability patching process?
4. According to your oral testimony before the House Energy and Commerce Committee on October 3, 2017, Equifax has 225 cybersecurity professionals. Please list the criteria that must be met in order for an individual to qualify as a "cybersecurity professional" at Equifax. What cybersecurity training are these individuals provided and does Equifax maintain and encourage ongoing cybersecurity training of its employees?
5. Do all of the 225 cybersecurity professionals work in Equifax's Security Department or do some of them work in other departments? If in other departments, please specify which departments.
6. Who at Equifax received the U.S. Department of Homeland Security, Computer Emergency Readiness Team's (US-CERT) notification concerning the need to patch the Apache Struts vulnerability?
7. What steps did the company take after receiving the US-CERT notification? Please respond in detail and describe every action that was taken, the date on which the action was taken, who took the action, and who in the company each person involved directly reported to.

8. In your testimony before the House Energy and Commerce Committee on October 3, 2017, you stated that the attack was made possible because of a human error. Please explain in detail what the error was, the position held by the person who committed the error, who in the company this person directly reported to, and which of the individuals involved were part of the company's 225 cybersecurity professionals.
9. On March 8, 2017, did Equifax have any protocols for responding to vulnerability notification from US-CERT and what actions should take place following a notification? If so, please explain the protocols in detail, including each task that was required to be completed, who was required to complete the task, who in the company these individual(s) had to directly report to, and any verification mechanisms that were supposed to be in place to check whether each task was completed. Please indicate what, if any, industry standards, guidelines, or best practices were used to develop these protocols.
10. What steps has the company taken to address previous errors regarding its patching process and to mitigate potential errors in the future?
11. In your testimony before the House Energy and Commerce Committee on October 3, 2017, you stated that a scanner failed to detect a vulnerability in the dispute portal. What scanning technology was your company using to scan this portal? Please respond in detail and include the name of the vendor, software, and service offering if applicable.
12. When did Equifax begin using this particular vendor and software to scan the dispute portal? Is the company still using the vendor and software to scan this portal?
13. Who at Equifax conducted the scans on March 15, 2017 and who did the individual(s) directly report to in the company?
14. How frequently does Equifax conduct vulnerability scans of its dispute portal?
15. What circumstances dictate whether a scan of the dispute portal is conducted?
16. How many scans were conducted of the dispute portal between March 8, 2017 and July 29, 2017? Please provide a list of the dates on which the scans were conducted.
17. Between March 8, 2017 and July 29, 2017, was any other scanning technology used to scan the dispute portal for potential vulnerabilities besides the scanning technology that was used on March 15, 2017? If so, please list the vendor, software, and service offering if applicable.
18. Did Equifax experience any problems with the scanning technology that was used on March 15, 2017 prior to this date?
19. Is the scanning technology that was used to conduct the scans on March 15, 2017 used to scan any of Equifax's other portals? If so, please specify the names of the portals.
20. What type of training on using scanning technology does Equifax provide to the individuals who conduct the vulnerability scans? How many individuals who conduct the scans in the company receive this training? Does the company consider these individuals to be a part of its 225 cybersecurity professionals?

21. On March 15, 2015, did Equifax have any protocols in place for conducting vulnerability scans or for measuring the effectiveness of the scans? What, if any, industry standards, guidelines, or best practices were used to develop these protocols?
22. On March 15, 2017, what were Equifax's internal reporting requirements following vulnerability scans of its portals? What, if any, industry standards, guidelines, or best practices were used to develop these requirements?
23. Since discovering the cyberattack, has the company made any changes with respect to how it conducts vulnerability scans and what technology it uses, particularly as it relates to the dispute portal and any other portals that contain consumer data?
24. Is Equifax a member of or does it participate in any of the Department of Homeland Security Sector Coordinating Councils? If not, do you believe that companies such as Equifax could benefit from participating in such efforts?