

1 NEAL R. GROSS & CO., INC.

2 RPTS SHIPLE

3 HIF276170

4
5
6 OVERSIGHT OF THE EQUIFAX DATA BREACH:

7 ANSWERS FOR CONSUMERS

8 TUESDAY, OCTOBER 3, 2017

9 House of Representatives

10 Subcommittee on Digital Commerce and Consumer

11 Protection

12 Committee on Energy and Commerce

13 Washington, D.C.

14
15
16
17 The subcommittee met, pursuant to call, at 10:00 a.m., in
18 Room 2123 Rayburn House Office Building, Hon. Robert Latta
19 [chairman of the subcommittee] presiding.

20 Members present: Representatives Latta, Harper, Burgess,
21 Upton, Lance, Guthrie, McKinley, Kinzinger, Bilirakis, Bucshon,
22 Mullin, Walters, Costello, Walden (ex officio), Schakowsky,
23 Lujan, Clarke, Cardenas, Dingell, Matsui, Welch, Kennedy, Green,
24 and Pallone (ex officio).

25 Also present: Representatives Barton, Murphy, Carter,

1 Degette, Tonko, and McNerney.

2 Staff present: Jennifer Barblan, Chief Counsel, Oversight
3 & Investigations; Ray Baum, Staff Director; Karen Christian,
4 General Counsel; Kelly Collins, Staff Assistant; Zachary
5 Dareshori, Staff Assistant; Jordan Davis, Director of Policy and
6 External Affairs; Melissa Froelich, Chief Counsel, Digital
7 Commerce and Consumer Protection; Adam Fromm, Director of
8 Outreach and Coalitions; Ali Fulling, Legislative Clerk,
9 Oversight & Investigations, Digital Commerce and Consumer
10 Protection; Theresa Gambo, Human Resources/Office Administrator;
11 Elena Hernandez, Press Secretary; Zach Hunter, Director of
12 Communications; Bijan Koochmaraie, Counsel, Digital Commerce and
13 Consumer Protection; Alex Miller, Video Production Aide and Press
14 Assistant; Mark Ratner, Policy Coordinator; Dan Schneider, Press
15 Secretary; Sam Spector, Policy Coordinator, Oversight &
16 Investigations; Madeline Vey, Policy Coordinator, Digital
17 Commerce and Consumer Protection; Hamlin Wade, Special Advisor,
18 External Affairs; Jessica Wilkerson, Professional Staff,
19 Oversight & Investigations; Everett Winnick, Director of
20 Information Technology; Greg Zerzan, Counsel, Digital Commerce
21 and Consumer Protection; Michelle Ash, Minority Chief Counsel,
22 Digital Commerce and Consumer Protection; Priscilla Barbour,
23 Minority Energy Fellow; Jean Fruci, Minority Energy and
24 Environment Policy Advisor; Rick Kessler, Minority Senior Advisor
25 and Staff Director, Energy and Environment; Alexander Ratner,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Minority Policy Analyst; and Tuley Wright, Minority Energy and
2 Environment Policy Advisor.

1 Mr. Latta. Good morning. The Subcommittee on Digital
2 Commerce and Consumer Protection will come to order. The chair
3 now recognizes himself for 5 minutes for an opening statement.

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

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

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

25 In this case, sensitive personal information that is used

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 to build credit histories and allow individuals to engage in
2 commerce, open credit cards, buy cell phones and appliances, and
3 secure mortgages has been compromised. Reasonable security
4 measures must be implemented, practiced, and continually improved
5 by companies that collect and store data in order to guard against
6 unauthorized access to sensitive personal information.

7 Otherwise, consumers will face substantial financial harm.

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

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

25 This is a staggering amount of sensitive personal

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 information and impacts an extraordinary number of credit-visible
2 Americans that is in the hands of criminals that could result in
3 fraud or identity theft. We need these numbers confirmed.

4 Today, we must understand the following: First, how did the
5 hackers get into Equifax's system for so many weeks and pull so
6 much information out of the system without being detected?

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

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

22 I believe the American public deserves to know the facts
23 about when and how Mr. Smith, company management, and the board
24 of directors were made aware its systems were vulnerable to
25 hackers and how over 143 million sensitive personal data records

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 were stolen. To that end, what were the steps taken and in what
2 timeframe to notify and help individuals that were impacted? I
3 look forward to getting these answers today and many more
4 questions for the American people answered this morning.

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

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

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

20 Because consumers don't have a choice, we can't trust credit
21 reporting agencies to self-regulate. It is not like when you get
22 sick at a restaurant and decide not to go there anymore. Equifax
23 collects your data whether you want to have it collected or not.
24 If it has incorrect information it is really an arduous process
25 -- I have tried it -- to get it corrected. When it comes to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 information security you are at the mercy of whatever Equifax
2 decides is right and once your information is compromised the
3 damage is ongoing.

4 Given vast quantities of information and lack of
5 accountability, a major breach at Equifax I would say would be
6 predictable if not inevitable. I should really say breaches.
7 This is the third major breach Equifax has had in the past 2 years.
8 From media reports and the subcommittee's meeting with Equifax
9 officials after the breach, it is clear to me that the company
10 lacked appropriate policies and practices around data security.

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

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

23 The response to the breach was its own debacle. Equifax
24 offered consumers credit monitoring services that initially came
25 with a mandatory arbitration clause which fortunately has been

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 corrected; Equifax tweeted links to the wrong URL directing
2 victims to a fake website; the call center was understaffed; and
3 in the end Equifax has had to apologize for its supposed breach
4 response almost as much as it has apologized for the breach itself.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

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

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

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

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

22 Mr. Chairman, the Energy and Commerce Committee have always
23 tried to put our consumers first in everything we do on public
24 policy. So today we will begin to get the answers for the public,
25 hold Equifax accountable, and make clear that businesses holding

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 America's most sensitive data have a responsibility under
2 existing laws to protect those data. Today gives whole new
3 meaning to Mr. Smith Goes To Washington. It is not a run on the
4 bank that is at issue, it is a run on financial records of 145
5 million Americans. And the consequences and the inconveniences
6 for our fellow citizens is every bit as important to discuss today
7 as the reasons behind why this breach occurred in the first place.

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

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

25 While there are still many questions that need answers, a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 few details have emerged. First, the vulnerability that the
2 hackers used to get into the Equifax system was discovered in early
3 March. From the beginning, the vulnerability was described as
4 critical and easily exploitable. That information was pushed out
5 through multiple security information sharing channels including
6 by the U.S. Computer Emergency Readiness Team to Equifax's chief
7 security officer.

8 For some period of time between March and August of 2017,
9 the hackers were able to sit on Equifax's system and siphon out
10 145 million records without being detected. How did this go
11 unnoticed? Further, is there a process in place to raise flags
12 or alarms when massive amounts of data are pulled out of the
13 Equifax system?

14 Then there are questions about Equifax's response for
15 consumers that we need answers to. Why was the consumer-facing
16 website created on a separate domain from the main Equifax
17 website? Did anyone raise concerns about creating more consumer
18 confusion with a separate website? Are consumers able to sign
19 up for the products offered by Equifax today? How many consumers
20 have placed a fraud alert on their account or frozen their credit?

21 And on top of all the other issues, multiple times Equifax
22 tweeted the wrong URL directing consumers to the wrong website
23 to check if they were part of a breach. Talk about ham-handed
24 responses, this is simply unacceptable and it makes me wonder
25 whether there was a breach response plan in place at all and if

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 anyone was in charge of overseeing and executing that plan. I
2 have to agree with the interim CEO when he said there is
3 insufficient support for consumers.

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

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

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

24 It has been 4 weeks since the breach was made public and at
25 least 10 weeks since it was discovered by Equifax's employees,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 yet Equifax's customer service has been confusing and unhelpful.
2 Equifax even tweeted a link to a fake website. Many of the
3 remedies Equifax is now offering to consumers were not offered
4 upfront or in good faith. They were forced out of the company
5 only after a public outcry and they are still inadequate.

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

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

23 Consumers do not have any say in whether or not the Equifax
24 collects and shares their data and that is what makes this breach
25 so concerning. This is unlike other breaches at stores such as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Target and Michael's where consumers could make a choice and
2 change their shopping habits if they were upset with how the
3 companies protected data. That is simply not the case with
4 Equifax.

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

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

23 Mr. Lujan. Thank you to our ranking member, Mr. Pallone,
24 and I thank the committee's leadership for organizing this
25 important hearing. 145,500 thousand million Americans, 145.5

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 million people at risk because of Equifax's failure. Now Mr.
2 Smith, the American people deserve answers and I hope you are
3 prepared to provide them. Not just about what caused the breach,
4 but what Equifax is doing to prevent this from happening again
5 and to ensure that those who were harmed are made whole.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

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

3
4 Mr. Smith. Thank you. Chairman Walden, Ranking Member
5 Pallone, Chairman Latta, Ranking Member Schakowsky, and the
6 honorable members of the subcommittee, it is an honor to be here
7 before you today.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 is ongoing.

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

8 On July 29th and July 30th, suspicious activity was detected
9 and a team followed our security incident protocol. The team
10 immediately shut down the portal and began our internal security
11 investigation. On August 2nd, we hired top cybersecurity
12 forensic and legal experts and at that time we notified the FBI.
13 At that time, to be clear, we did not know the nature or the scope
14 of the incident. It was not until late August that we concluded
15 that we had experienced a major breach.

16 Over the weeks leading up to September 7th, our team
17 continued working around the clock to prepare. We took four steps
18 to protect consumers. Step number one, determining when and how
19 to notify the public, relying on the advice of our experts that
20 we needed to have a plan in place as soon as we announced. Step
21 two, helping consumers by developing a website, staffing up
22 massive call centers, and offering services free to every
23 American. Three, preparing for increased cyber attacks which we
24 were advised by the cybersecurity experts that we should expect.
25 And finally, continue to coordinate with the FBI and their

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 criminal investigation of the hackers and also to notify other
2 federal and state agencies.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

16 [The prepared statement of Mr. Smith follows:]

17
18 *****INSERT 1*****

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

8 Mr. Smith, the timeline of events is raising some red flags
9 I would like to ask you about. According to your statement, the
10 first time you heard about the breach of security was on July the
11 31st of 2017; is that correct?

12 Mr. Smith. Yes, Congressman. That is correct.

13 Mr. Latta. And you first asked for a briefing about the
14 breach on August the 15th; is that correct?

15 Mr. Smith. Yes. That is correct.

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

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

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

25 Mr. Smith. That is correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

25 Mr. Latta. Well, let me just back up to July the 31st when

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 you learned, again you were talking with the experts at that time
2 and you learned about the breach and you testified that you did
3 not know that personal information had been stolen at that point.
4 But did you ask anyone if personal information had been stolen
5 when you found out about that breach?

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

12 Mr. Latta. Okay, so I guess again, but again not knowing
13 if that information, if that personal information had been stolen
14 at that time, you know, your company is built on data and at any
15 point did you think it was important of if somebody in the company
16 started looking at if personal data had been stolen at that point?

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 he notify you of the breach?

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

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

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

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

17 Mr. Smith. Again it is important to say on July 31st we did
18 not know it was a breach at that time, suspicious activity only.
19 The first notification to the board was the lead director on the
20 22nd of August, which followed in the chronology of events a
21 meeting I had with our cybersecurity experts and our outside
22 counsel had occurred on the 17th of August. That is when the
23 picture was starting to develop.

24 Mr. Latta. Thank you. My time is expired and I will
25 recognize the gentlelady from Illinois, the ranking member, for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 5 minutes.

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

7 Mr. Smith. That is correct, Congresswoman.

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

10 Mr. Smith. Correct.

11 Ms. Schakowsky. Okay. So we were told that Mr. Kelley was
12 informed by the chief security officer the week of July 30th --
13 we have just been talking about that -- that a cybersecurity
14 incident you mentioned that had occurred; is that correct?

15 Mr. Smith. He was notified, it is my understanding, on the
16 31st of July.

17 Ms. Schakowsky. 31st, okay.

18 Mr. Smith. That there was suspicious activity in a
19 particular environment called a web portal that was a dispute
20 environment.

21 Ms. Schakowsky. We were told that Mr. Kelley -- this is our
22 staff -- was informed at the same time that the incident might
23 have compromised personally identifiable information; is that
24 correct?

25 Mr. Smith. The only knowledge I have is he was notified on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 the 31st that there was suspicious activity in a consumer dispute
2 portal.

3 Ms. Schakowsky. Well, we were told that Mr. Kelley then
4 wrote a short memo to you regarding the incident; is that correct?

5 Mr. Smith. Correct, Congresswoman. And in his email it
6 said some suspicious activity.

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

13 Mr. Smith. Yes. Mr. Kelley who is our general counsel owns
14 the clearance process and he would --

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

17 Mr. Smith. Yes.

18 Ms. Schakowsky. Did anyone of these three executives have
19 knowledge the cybersecurity incident had occurred?

20 Mr. Smith. To the best of my knowledge, Congresswoman, no.

21 Ms. Schakowsky. When were they informed that the incident
22 had occurred?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

7 Mr. Smith. Congresswoman, I would come back to it again,
8 he did not know it was a breach when he approved --

9 Ms. Schakowsky. That it could have been a breach.

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

12 Ms. Schakowsky. What the heck does suspicious -- it could
13 be a breach, right?

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

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

20 Mr. Smith. That is correct.

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

24 Mr. Smith. That is correct.

25 Ms. Schakowsky. Retiring, which is the category right now

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 although the company maintains the right to change that
2 designation, also means you will be free to sell your Equifax stock
3 which is worth about \$24 million; is that correct?

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

10 Ms. Schakowsky. And that is in addition to Equifax stock
11 you sold earlier in this year for \$19 million; is that correct?

12 Mr. Smith. That sounds correct.

13 Ms. Schakowsky. And according to one report, you could be
14 eligible for \$22 million in performance-based compensation
15 depending how Equifax stock performs in the next 3 years; is that
16 right?

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

23 Ms. Schakowsky. I was just informed by staff that the chief
24 security officer told the chief legal officer verbally that there
25 was PII that according to a call with staff yesterday that actually

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 there was a mention of the breach of personally identifiable
2 information. The CSO told that -- yes, told us in a call yesterday
3 is what I just heard from staff.

4 Mr. Smith. Congresswoman, I have no documentation, no
5 insight, no knowledge that anyone in the company had informed me
6 or in that case the chief security officer -- or the chief general
7 counsel that there was a breach on July 31st. Is that what you
8 said?

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

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

17 The Chairman. Thank you, Mr. Chairman.

18 Mr. Smith, thanks again for being here today. As you know,
19 this is an example of an Equifax credit report in my hand. It
20 lists Social Security Numbers, address, credit history, debts,
21 all the sort of personal financial information. It is the
22 lifeblood of Equifax, right? I mean these data points are really,
23 really important to what you do as a company?

24 Mr. Smith. Congressman, that is correct.

25 The Chairman. It is a \$3 billion company, data on 820

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 million customers worldwide, and yet it appears this breach
2 happened because the company didn't know it was running certain
3 software on its system, right, the Apache Struts software that
4 had the patch requirement?

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

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

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

23 The Chairman. Okay, so then people ask us how does that
24 happen? If as a sophisticated of a company as you headed is with
25 so much at risk, how does this happen? And, you know, we have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 colleagues that say we are going to double the fines, triple the
2 fines, put fines in, do all these things, but how does this happen
3 when so much is at stake? I don't think we can pass a law that
4 excuse me for saying this but fix a stupid, I can't fix stupid
5 as a colleague of mine used to say. With so much at risk -- I
6 have talked to other software companies and people in this space
7 who say some companies have an automated system that when a patch
8 comes out it automatically gets installed. That is not what you
9 had necessarily, right?

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

14 The Chairman. Right.

15 Mr. Smith. They follow the protocol which is to notify the
16 appropriate people within the timeframe that the protocol called
17 for. Unfortunately, the human error was they did not find the
18 patch. Did not know --

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

23 Mr. Smith. Congressman, great question, if I may clarify.

24 The Chairman. Yes, please.

25 Mr. Smith. The human error was the individual who is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 responsible for communicating in the organization to apply the
2 patch did not.

3 The Chairman. So does that mean that that individual knew
4 that the software was there and it needed to be patched and did
5 not communicate that to the team that does the patching? Is that
6 the heart of the issue here?

7 Mr. Smith. That is my understanding, sir.

8 The Chairman. And there is no, you know, I was on a bank
9 board for awhile and, you know, we always had sort of double checks
10 on everybody, right. Do you not have a double check of some sort,
11 an audit of some sort? Is there -- it seems like that was a single
12 point.

13 Mr. Smith. The double check was the scanning device that
14 was deployed a few days later.

15 The Chairman. But did the scanning device -- I don't know
16 how that process works. Does it know you have that software or
17 do you have to tell it that is what you are scanning for?

18 Mr. Smith. It is the latter. You have got to tell it what
19 it is looking for. It scans the environment looking for --

20 The Chairman. And so the individual who didn't tell the IT
21 team -- I will call it the IT team, whatever, the security team
22 -- that is where the individual failed. Was that the same person
23 telling them what to look for?

24 Mr. Smith. No. The scanner is deployed by the security
25 team. And I should clarify there that the rationale or the reason

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 why the scanner or the technology piece did not locate the
2 vulnerability is still under investigation by outside counsel.

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

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

15 The Chairman. But to the point that the head of your
16 security team comes to you and says, hey, we have another one?

17 Mr. Smith. Oh. That is not uncommon. It is not uncommon.

18 The Chairman. How often would that happen in the course of
19 a week that they would come to the CEO and say heads up?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The Chairman. Thank you for the indulgence on the
2 committee. I yield the balance of my time.

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

6 Mr. Pallone. Thank you.

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

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

18 Mr. Pallone. August 11th, initially, and then August 17th
19 in the second speech.

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

23 Mr. Pallone. Well, I am just -- yes. I mean on the 17th
24 you said in a speech, fraud is a huge opportunity for Equifax.
25 It is a massive growing business for us. I am just looking for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 a number. At the time, roughly, how many consumers did you
2 believe had been compromised by the breach?

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

18 Mr. Smith. Congressman, we are trying to change the
19 paradigm, and what I mean by that is this will be in an environment
20 viewed as a service, a utility not a product. But we know
21 cross-selling, up-selling, or any products available to the
22 consumer, when they go to get and sign up for the lock product
23 it is a service to them and that is the only product the service
24 will be able to get.

25 Mr. Pallone. Now will Equifax give consumers an easy and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 free method to choose not to share their data in this way, even
2 if the consumer already has a business relationship with the third
3 party?

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

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

15 Mr. Smith. Congressman, a couple of differences. Number
16 one, the product we offer today for consumers protects the
17 consumer at the same level of protection they would get January
18 31st. The difference is today it is a browser-enabled product
19 or service. The 31st of January it will be an application, much
20 simpler and easier for the consumer to use. The protection is
21 largely the same.

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

25 Mr. Pallone. I guess, you know, the difference other than

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 not expiring between the credit report lock that is part of
2 TrustedID Premier and the credit locking tool that will be
3 available in January, why not just extend the freeze program?

4 Mr. Smith. There is a difference between the freeze product
5 which came to pass with FACTA back in 2003, passed into law in
6 2004. That is now governed by state laws in all states and it
7 is a cumbersome process for a consumer. In many cases, some
8 states require you to mail in your request for a freeze and then
9 we must mail you a PIN, so your ability to get access to get credit
10 when you want credit is encumbered.

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

17 Mr. Pallone. My time has run out, Mr. Chairman.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Smith. Congressman, last time I checked it is somewhere
2 close to 13 billion.

3 Mr. Barton. 13 billion. I am told by my staff that this
4 current, this latest data breach was about 143 million people;
5 is that right?

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

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

23 Mr. Smith. Congressman, I understand your question. I
24 think the path that we were on when I was there and the company
25 has continued is the right path, and that is the path of allowing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the consumers to control the power of who and when accesses their
2 credit file going forward, taking the --

3 Mr. Barton. Well, the consumer can't control the security
4 of your system.

5 Mr. Smith. That is true, sir. But they can control --

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

13 But I am tired of almost every month there is another security
14 breach and it is okay, we have to alert you. I checked my file
15 to see if I was one of the ones that got breached, and apparently
16 I wasn't. I don't know how I escaped, but I didn't get breached.
17 But my staff person did, and we looked at her reports last night
18 and the amount of information that is collected is way beyond what
19 you need to determine if she is creditworthy for a consumer loan.

20 Basically, her entire adult history going back 10 years
21 everywhere she has lived, her name, her date of birth, her Social
22 Security Number, her phone numbers, her addresses, her credit
23 card, student loans, security clearance applications for federal
24 employment, car insurance, even employment history of jobs that
25 she worked when she was in high school. That is not needed to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 determine whether she is worthy of getting a \$5,000 credit card
2 loan or something and now it is all out in the netherworld of
3 whoever hacked it.

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

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

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

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

22 Mr. Lujan. Thank you, Mr. Chairman.

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

25 Mr. Smith. Congressman, there is a process. It is a little

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 different, but as far as the consumer and the protection that he
2 or she would get from doing one versus the other is virtually if
3 not exactly the same.

4 Mr. Lujan. Well, virtually almost exactly is not the same.
5 Are they different?

6 Mr. Smith. It is the same.

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

8 Mr. Smith. As far as the protection --

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

13 Mr. Smith. You are referring to the freeze or the lock?

14 Mr. Lujan. You said they are the same so.

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

18 Mr. Lujan. And that also extends to Experian and
19 TransUnion?

20 Mr. Smith. No, sir. It does not.

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

25 Mr. Smith. Congressman, the company has come out with what

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 they feel is a comprehensive five different services today and
2 a lifetime lock. I would encourage, to be clear, I would
3 encourage TransUnion and Experian to do the same. It is time we
4 changed the paradigm, give the power back to the consumer to
5 control who accesses his or her credit data. It is the right thing
6 to do.

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

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

17 Mr. Lujan. Mr. Smith, will those comprehensive sets of
18 products make consumers whole?

19 Mr. Smith. It will protect them going forward.

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

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

23 Mr. Lujan. If someone's credit has been stolen and someone
24 went and opened up a bunch of their accounts, bought furniture,
25 bought cell phones, bought a bunch of fuel, and now this consumer

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 can't fix their history they have been harmed. In that case will
2 Equifax make that person whole?

3 Mr. Smith. Congressman, as I have said I apologize. We
4 have offered them a --

5 Mr. Lujan. Thank you very much, sir.

6 So I want to go back to the line of questioning earlier from
7 Mr. Pallone. On August 11th, in your prepared testimony it says
8 that you were aware of a large amount of consumer PII. On August
9 15th, it says in your prepared testimony a PII had been stolen,
10 it appeared likely, and that you requested a detailed briefing
11 to determine how much the company should proceed. On August 17th,
12 it says, you, I held a senior leadership meeting to receive the
13 detailed briefing on the investigation. You gave a speech also
14 on the 17th about profiting off of fraud with these new markets.
15 You shared with Mr. Pallone that you were not aware of PII being
16 stolen. What is it?

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

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

23 Mr. Smith. I was not aware it was stolen. I was aware there
24 was --

25 Mr. Lujan. It says in your prepared testimony that you were

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 aware, that you asked for a detailed briefing to determine how
2 the company should proceed. So you were aware that PII was stolen
3 on the 15th; is that true or not true?

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

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

10 Mr. Smith. On August 15th --

11 Mr. Lujan. Regardless of the amount were you aware of that?

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

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

19 Mr. Smith. Yes, he is.

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

24 Mr. Smith. There is an investigation going on by the board
25 at this time.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

19 Mr. Harper. Thank you, Mr. Chairman.

20 Mr. Smith, thank you for being here to testify today. In
21 your written testimony and in response to some of the chairman's
22 questions, you stated that you were informed of suspicious
23 activity on July the 31st by your chief information officer and
24 went on to discuss that. And you said, I certainly did not know
25 that personal identifying information, PII, had been stolen or

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 have any indication of the scope of the attack. Did you ask him
2 if there had been any personal identifying information that had
3 been obtained?

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

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

11 Mr. Smith. No, I did not.

12 Mr. Harper. Were you made aware at that point of the Apache
13 Struts patch?

14 Mr. Smith. No, sir. I was not.

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

18 Mr. Smith. No, Congressman. I did not.

19 Mr. Harper. Had you had any meetings with them about any
20 other security information during that time from March until July
21 31st?

22 Mr. Smith. Oh yes. We would have routine meetings,
23 security reviews, IT reviews.

24 Mr. Harper. How often do you have those?

25 Mr. Smith. Common due process would be at least quarterly.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

5 Mr. Smith. Make sure I understand your question. Why
6 didn't --

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

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

11 Mr. Harper. Well, how many do you remember? Do you
12 remember any of those?

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

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

21 Mr. Smith. No, sir. I did not.

22 Mr. Harper. All right. In your testimony you indicate that
23 the security department ran scans in March for the vulnerability
24 but failed to identify it. Can you explain how this is possible
25 and why was there never any confirmation of anybody coming back

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 and checking to see, okay, we have this identified information,
2 there was a failure of someone on the team to identify this that
3 it was being used, that the software was even being used? Was
4 there no one coming in to verify that? Do you have any outside
5 person prior to the ones that you hired to look at this?

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

10 Mr. Harper. You said this individual?

11 Mr. Smith. Yes.

12 Mr. Harper. So you had one person responsible for this?

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

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

22 Mr. Smith. No, sir.

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

25 Mr. Smith. We have for years, sir, yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Harper. Okay. So it just appears, obviously, I mean
2 the job wasn't done and so we know that and we are trying to look
3 at this. And I know too there was an Equifax spokeswoman who said,
4 we have taken short-term mediation steps and continue to implement
5 and accelerate long-term security improvements as part of ongoing
6 actions to help prevent this type of incident from happening
7 again.

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

10 Mr. Smith. Worldwide?

11 Mr. Harper. Yes, sir.

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

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

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

23 Mr. Harper. You know, my home state of Mississippi has three
24 million people, three million people. Almost 1.4 million files
25 have been breached in my state. If you take away people that are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 minors who don't have a file yet, almost my entire state is going
2 to be impacted. So this is a travesty, something that was
3 preventable, we know, and so saying that we want to protect what
4 goes forward doesn't bring us a lot of comfort today. Thank you
5 and I yield back.

6 Mr. Latta. The gentleman yields back. The chair now
7 recognizes the gentleman from California for 5 minutes.

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

11 Mr. Smith, welcome to Washington. Are you currently
12 employed by Equifax?

13 Mr. Smith. No, sir.

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

19 Mr. Smith. I believe I was asked specifically to come before
20 the committee.

21 Mr. Cardenas. By Equifax or the committee?

22 Mr. Smith. My understanding is by the committee.

23 Mr. Cardenas. Okay. Okay. Apparently the committee
24 asked for the CEO at the time and at that time you were still the
25 CEO, but you are no longer the CEO. Did you inquire as to why

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 the current CEO or interim CEO didn't come before this committee?

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

6 Mr. Cardenas. Thank you. I get the picture. On August
7 31st or, excuse me, on July 31st you were notified of the
8 suspicious activity that eventually as we now know was a 145
9 million person breach? Was it July 31st, was it?

10 Mr. Smith. Yes, Congressman. It was a brief interaction
11 --

12 Mr. Cardenas. A verbal interaction?

13 Mr. Smith. With -- yes.

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

17 Mr. Smith. A point of clarification, I was notified on the
18 31st of July by the chief information officer, Dave Webb, in a
19 very brief interaction that this portal seemed to have a
20 suspicious incident. There was a communication trail internally
21 between others that also referenced that I was aware of this
22 incident through my interaction with Dave Webb.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Smith. That is my recollection.

2 Mr. Cardenas. Okay. Mr. Chairman, is it appropriate for
3 this committee to ask for that trail of documents?

4 Mr. Latta. I would ask the -- for our counsel, but I would
5 say --

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

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

15 Mr. Smith. That is correct.

16 Mr. Cardenas. And then there is another higher-up that is
17 no longer --

18 Mr. Smith. The chief security officer.

19 Mr. Cardenas. Okay, chief security officer. However, the
20 then, John Kelley, chief legal officer, was the chief legal
21 officer at that time but still is currently the chief legal
22 officer, correct?

23 Mr. Smith. That is correct.

24 Mr. Cardenas. Okay. Apparently, the chief legal officer
25 on or about, between July 29th and August 1st went to outside

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 counsel and hired outside counsel who -- correct?

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

6 Mr. Cardenas. Okay, thank you. When executives at Equifax
7 want to sell stock they need to get the chief legal officer to
8 sign off?

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

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

16 Mr. Smith. That is correct, sir.

17 Mr. Cardenas. Okay. And apparently they did get the okay?

18 Mr. Smith. Yes. That is my understanding.

19 Mr. Cardenas. And you were the CEO at the time that they
20 sold that stock?

21 Mr. Smith. And I have no step in that --

22 Mr. Cardenas. I get it.

23 Mr. Smith. Yes. I was --

24 Mr. Cardenas. I am referring to John, but you were the CEO
25 at the time.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

16 Mr. Upton. Thank you, Mr. Chairman.

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

23 Here is an Equifax credit report for somebody that I know.
24 It is 131 pages long, unbelievable in terms of the data that has
25 been collected on this particular individual. I would guess that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 most individuals have no clue that there is that much data that
2 has been assembled on their own personal family account.

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

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

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

21 Regardless of self-employed income, regardless of automated
22 underwriting findings, when self-employed income is used to
23 qualify, the following documentation is required: most recent 2
24 years of their individual tax returns with all schedules and W-2s
25 and K-1s; most recent 2 years' business returns; IRS forms 1120

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 and 1120S; 1065s in which the borrower has ownership interest at
2 25 percent or more; and a complete and signed IRS form 4506-T is
3 required for every borrower on the loan application; tax
4 transcripts validated from the IRS are required for each year
5 documented in the loan file.

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

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

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

23 Mr. Upton. The last question I have is how did you know,
24 I mean how -- we have had a lot of hearings, a number of them
25 classified. Breaches made into Department of Energy, utilities,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 a whole number of different major players where hackers are coming
2 in trying to break and penetrate daily. What tripped these guys
3 up? What was the -- how did you identify in fact a breach had
4 been made? What was their mistake?

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

11 Mr. Upton. Yield back, my time is expired.

12 Mr. Latta. Thank you very much. The gentleman yields back
13 and the chair now recognizes the gentelady from Michigan for 5
14 minutes.

15 Mrs. Dingell. Thank you, Mr. Chairman.

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

21 But I want to ask a few questions about where we go from here,
22 because I hope this has awoken the American consciousness about
23 privacy and credit that they need to be paying far more attention
24 to. This breach is different than most. Not only the scale of
25 those affected but the type of information taken. In the past,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 folks usually just changed your passwords, maybe you got a new
2 credit card and that was it. You know, it was an annoyance but
3 it had no real impact on your life.

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

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

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

23 Mrs. Dingell. I don't think it is all the same, but thank
24 you. After your security department blocked the suspicious
25 traffic you mentioned in your testimony, did anyone from your team

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 or outside companies venture beyond the parameter of your network
2 to attempt to locate where they came from?

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

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

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

21 Mr. Smith. Congresswoman, I think we can help. I think we
22 can help by the announcement of this offering to all Americans
23 the ability to lock and unlock your credit file for life for free.
24 There needs to be a greater awareness, I understand your point
25 clearly. And I think by making this available to all Americans

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 is one step in doing that.

2 Mrs. Dingell. So I was just actually even educating my
3 colleagues up here about Credit Karma and they were stunned by
4 how easy it was with two little factoids to suddenly unleash the
5 amount of money they had in every one of the credit card companies,
6 what any data inquiries have been, and all of the different
7 factors. I have a couple -- and I think most people don't
8 understand that it is not just you, but Experian and TransUnion
9 who are also collecting this data. Why do consumers have
10 to pay you to access their credit report? Why should that data
11 not be free?

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Lance. Thank you, Mr. Chairman.

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

5 Mr. Smith. Congressman, it is possible but at this time --

6 Mr. Lance. It is possible. Number two, is it possible it
7 is the government of another country?

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

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

12 Mr. Smith. Congressman, I will defer that. We have the FBI
13 involved.

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

16 Mr. Smith. I have no opinion.

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

23 Mr. Smith. Congressman, a few points here of clarification.
24 The stock was sold on the 1st and the 2nd. So --

25 Mr. Lance. Yes, I said the 2nd. Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

2 Mr. Lance. Yes.

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

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

10 Mr. Smith. Yes.

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

13 Mr. Smith. Congressman, I have known these individuals for,
14 some of them up to 12 years. They are honorable men. They are
15 men of integrity. They followed due process. They went through
16 the clearance process through the general counsel. I have no
17 indication that they had any knowledge of the breach at the time
18 they made the sale.

19 Mr. Lance. Did you have knowledge of the breach at that
20 time?

21 Mr. Smith. I did not, sir.

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

24 Mr. Smith. I was notified on July 31st in a conversation
25 with the chief information officer that there was suspicious

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 activity detected in an environment called the web portal for
2 consumer dispute. No indication of a breach.

3 Mr. Lance. That was prior to the sale of the stock; is that
4 accurate?

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

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

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

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

22 Mr. Smith. Congressman, I don't have the exact number, but
23 as I said in my opening testimony I apologize for that startup.
24 It was overwhelming in volume, overwhelming. I think I mentioned
25 over 400 million U.S. consumers coming to a website in 3 weeks.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 We went live in a very short period of time with call centers.
2 Our two larger call centers were taken down in the first few days
3 by Hurricane Irma. The team is committed and was committed to
4 make the experience better for the consumer and I am told that
5 each and every day that the process is getting better.

6 Mr. Lance. On August 22nd, you notified a lead director,
7 Mr. Fiedler -- I hope I am pronouncing that right -- of the data
8 breach, and the full board was informed later, I believe 2 days
9 later. Why was there nearly a week between August 17th and August
10 22nd before members of the board were alerted?

11 Mr. Smith. Congressman, the picture was very fluid.

12 Mr. Lance. Fluid, fluid. What does that mean?

13 Mr. Smith. We were learning new pieces of information each
14 and every day. As soon as we thought we had information that was
15 of value to the board I reached out to the lead director as you
16 said, Mark Fiedler, on the 22nd, convened a board meeting on the
17 24th. Convened a second board meeting on the 25th and had
18 subsequent board meetings routinely, if not daily in many cases,
19 through as recently as last week.

20 Mr. Lance. Thank you. And my time has expired, Mr.
21 Chairman.

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

25 Ms. Matsui. Thank you, Mr. Chairman, and thank you, Mr.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Smith, for appearing here today.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 residents notified of the breach as required?

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

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

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

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

17 Mr. Smith. Could you please repeat the question?

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Smith. The intent, if you will, of the solution we have
2 recommended, we implement, and are going live with in January of
3 2018, is in fact to give you as the consumer through this lock
4 product for life, for free, the ability to control who accesses
5 your personal information and who does not.

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

7 Ms. Matsui. Okay. So you currently offer a credit lock
8 product now and you plan to offer this other one for free starting
9 the end of January. And can you describe for me why you consider
10 that -- would a lock be more economical for you or would a freeze
11 be? I am trying to get the sense of the difference, because I
12 think there is a difference here.

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

21 Ms. Matsui. Okay. I have more questions but I know I have
22 run out of time. Thank you.

23 Mr. Latta. Thank you very much. The gentleman from
24 Illinois is recognized for 5 minutes.

25 Mr. Kinzinger. Thank you, Mr. Chairman, and sir, thank you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 for being here today.

2 This is obviously a huge issue, 145-1/2 million people
3 affected by this data breach. It is nearly half of all Americans.
4 That is a failure on multiple levels. It is a failure to keep
5 consumer personal information secure. It is a failure to
6 appropriately respond to a breach and a failure to notify the
7 public and much more. My constituents and the American people
8 need not just answers but they want assurances that they are not
9 going to be financially ruined by this.

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

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

24 Mr. Smith. Congressman, thank you for that question and I
25 want to clarify. The product offering that went live or the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 service offering on the 7th, it was never intended to have that
2 arbitration clause apply to this breach. It was a standard
3 boilerplate clause as a part of a product. As soon as we learned
4 that that boilerplate term was applied to this free service, I
5 think it was within 24 hours we removed that and tried to clarify
6 that. That was a mistake and one of the mistakes I alluded to
7 in my oral testimony about the remediation product on September
8 7th.

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

12 Mr. Smith. Not as it relates to the breach, Congressman.

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

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

17 Mr. Kinzinger. What is the reason for that?

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

20 Mr. Kinzinger. If you could get that to me that would be
21 good. Your press release indicates that the company has found
22 no evidence of unauthorized activity on Equifax's core consumer
23 or commercial credit reporting databases. What are Equifax's
24 core consumer and commercial credit reporting databases and how
25 are they distinct from the databases containing personal

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 information that was subject to the unauthorized theft?

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

8 Mr. Kinzinger. So in essence, were there 145.5 million
9 people that at one point had disputed credit issues then, if that
10 was the --

11 Mr. Smith. It is a portal they used and they could have been
12 in that portal for multiple reasons. And we also by regulation
13 have got to keep data for extended periods of time, in some cases
14 7-plus years. So it is a lot of data for a lot years, but it is
15 outside the core credit file itself.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

15 Mr. Kinzinger. Okay. And lastly, are your core consumer
16 or commercial credit reporting databases encrypted?

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

21 Mr. Kinzinger. Okay, so this wasn't but your core is?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Kinzinger. Okay, thank you, sir. I yield back.

2 Mr. Latta. Thank you very much. The gentleman yields back.

3 The chair now recognizes the gentleman from California for 5
4 minutes.

5 Mr. McNerney. I thank the chair for holding this hearing.

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

11 Mr. Smith. No, sir. This was the environment that had
12 deployed Struts.

13 Mr. McNerney. All right. That was a simple answer. You
14 might need to restart my time. In addition to Equifax's credit
15 monitoring and reporting services, the company has Equifax for
16 business offerings and in this capacity operates as a data broker.
17 As a part of these services the company collects large amounts
18 of data about consumers without consumers having any knowledge
19 of this happening. Was this information compromised in the
20 breach?

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

23 Mr. McNerney. Okay. Well, you are familiar with the
24 Equifax for business offerings?

25 Mr. Smith. Yes. We do have product offerings and solutions

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 for small businesses, medium sized businesses and large business
2 across the country, correct.

3 Mr. McNerney. Right. Was information from Equifax for
4 business also compromised in the breach?

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

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

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

19 Mr. McNerney. So what timeframe is that?

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

21 Mr. McNerney. So you say that you hired up to 250 personnel
22 to fix the issue?

23 Mr. Smith. I did not, the team did. I didn't hire them,
24 sir, but we now have a staff of 225 cyber or security experts around
25 the world. We made substantial investments over that timeframe.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 In the last 3 years alone we have invested approaching a quarter
2 billion dollars in security. There is an IBM benchmark. It says
3 financial service companies who tend to be best in class spend
4 somewhere between 10 and 14 percent of their IT budget in security.

5 Mr. McNerney. Well, they were notified of the -- I mean the
6 company was notified of the vulnerability in the Apache Struts
7 system days before the attack occurred.

8 Mr. Smith. Yes. We were notified by Department of Homeland
9 Security in March of 2017.

10 Mr. McNerney. And the attack occurred after the
11 notification?

12 Mr. Smith. Yes.

13 Mr. McNerney. So was there a human failure? I mean how
14 could 250 professionals that are designed and hired for that
15 purpose let a breach like that happen after they were notified?

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

24 Mr. McNerney. You mentioned that in your opening testimony.
25 That seems like a lack of competence or a professional error of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 some kind. What did you call it?

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

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

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

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

21 Mr. Smith. I have no opinion.

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

25 Mr. Smith. We, Congressman, offered five different

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 individual services, as you may or may not be aware, effective
2 September. One is the ability to monitor your credit files from
3 all three of us for free, another is to lock your file, another
4 is a dark web scanning product.

5 Mr. McNerney. That doesn't answer my question. How long
6 are we going to be vulnerable? How long are we going to -- our
7 Social Security Numbers are out there. This is forever, right?

8 Mr. Smith. Unfortunately, the number of breaches around a
9 Social Security Number has been on the rise as you know, and many
10 even this year. So there is another thought and that is, do we
11 think about how secure, really, is an SSN and is that the best
12 identifier for consumers going forward?

13 Mr. McNerney. Thank you, Mr. Chairman.

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

17 Mr. Guthrie. Thank you, Mr. Chairman.

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

25 And so not to repeat before, I heard you say that it was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 suspicious activity and therefore you didn't realize it was a
2 breach and then the action took place 3 weeks later when you did.
3 Looking back now, knowing how colossal this is and how big it is,
4 would you have done different? So from July 31st to August the
5 24th, what would you have done different that didn't happen or
6 Equifax didn't do?

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

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

25 Mr. Smith. Congressman, good question. It was strictly

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

10 Mr. Guthrie. Okay. According to reports, many consumers
11 weren't able to determine with certainty if their information was
12 breached. So why was Equifax unable to provide clarity or
13 certainty on whether individuals' information was breached?

14 Mr. Smith. When you went to the website, Congressman, and
15 you typed in six of your nine digits of your Social Security
16 Number, if it was likely that you were breached it would say
17 something along the lines of it looks like you may have been
18 compromised or breached as opposed to it is definite that you have
19 been breached, and that is because it was six digits versus nine.
20 The point is we offer this service, these five different services
21 to every American. It didn't matter if you were compromised or
22 not, every American was offered the same services.

23 Mr. Guthrie. So and just going forward, because we have to
24 also do an analysis and so what we are going to do as a legislative
25 body going forward to protect the American people. And what your

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 business does and what people in your business do are important
2 is when you can sit down at a car dealer, and I think you kind
3 of mentioned earlier, walk away with a car that afternoon because
4 somebody can check that you are creditworthy, and so having those
5 types of services are available.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 Mr. Smith. Thank you.

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

9 Mr. Bilirakis. Thank you, Mr. Chairman. I appreciate it.

10 Mr. Smith, one of my constituents accessed Equifax's
11 website, equifaxsecurity2017.com., to determine if they were
12 affected. They informed me that whether you submit your own
13 identifying information or whether you submit a random name and
14 Social Security Number you get the same message that you may be
15 affected. What course of action should consumers who haven't
16 received correspondence yet as to whether they are affected or
17 not, what is the course of action? And if they were affected what
18 are the next steps?

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

24 Mr. Bilirakis. Okay. I understand that Equifax currently
25 is waiving fees to freeze and unfreeze your credit. How long is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 that exemption going to stay in place because it is so very
2 important?

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

10 Mr. Bilirakis. Okay. As CEO, what level of involvement did
11 you have with regard to the data security and data protection?

12 Mr. Smith. Yes. The --

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

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

19 Mr. Bilirakis. Okay. What responsibilities did Ms.
20 Mauldin, again the chief security officer at Equifax at the time
21 of the breach, have with respect to data security, data
22 protection, and data breach notification? What were her
23 responsibilities?

24 Mr. Smith. Those were core to her responsibilities. She
25 was the head of cybersecurity and physical security in all 24

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 countries that we operate.

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

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

10 Mr. Bilirakis. Okay, so say a half dozen, a dozen?

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

12 Mr. Bilirakis. It would be a guess. More than three?

13 Mr. Smith. If it is important to you, Congressman, we can
14 find that information.

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

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

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

25 Mr. Smith. If I may just clarify again, on March 8th is when

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 the CERT came out saying there was a vulnerability in Apache
2 Struts. I was not even notified to put it in perspective that
3 there was an incident and didn't know what the incident was until
4 July 31st. So the number of meetings I would have with Dave Webb
5 would not have been related to this incident.

6 Mr. Bilirakis. All right, Mr. Chairman. Thank you, I yield
7 back.

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

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

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

15 Mr. Smith. Yes, Congressman.

16 Mr. Bucshon. Okay. So how does Equifax get the information
17 on people who have never directly associated with Equifax at all?
18 I mean I am not familiar with that.

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

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

25 Mr. Smith. Correct. As I define it we are part of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 federally regulated ecosystem that enables banks to loan money
2 to consumers.

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

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

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

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

22 Mr. Smith. I understand your point.

23 Mr. Bucshon. Yes. I also have a lot of constituents in
24 rural and lower income areas that may or may not have access to
25 the internet and WiFi. The penetrance of that it is interesting

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 depending on where you are of people who actually have WiFi and
2 the internet is not as high as you might think in rural America,
3 but some of those people still have probably applied for loans
4 and other things where their information could have been acquired
5 by your company.

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

12 Mr. Smith. Yes. Coming from Indiana I understand rural
13 Indiana.

14 Mr. Bucshon. There you go.

15 Mr. Smith. Congressman, we have set up the website that you
16 mentioned at a press release across the country. We have also
17 set up for those that don't have access to the web, to the internet,
18 call centers. We have staffed up. We have went from some 500
19 call center agents to over 2,700. So --

20 Mr. Bucshon. I guess that is again, I understand the call
21 centers and all that. I knew you had done that. But I guess that
22 is again making the assumption that people have watched the news
23 and know that there has been a breach and that they are proactive
24 in trying to find out whether they have been involved or not.

25 Is there any, other than a passive way for them to find out,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 is there anything proactive from Equifax's point of view that
2 might notify them that their data may have been compromised?

3 Mr. Bucshon. Well, in many states there is local
4 requirements, state requirements to take out advertisements in
5 newspapers and so forth. We follow those. One indication I did
6 mention earlier, it may or may not help those in rural Indiana,
7 but the visibility this has gotten is extremely high. I mentioned
8 400 and some odd million consumers had come to our website, so
9 it has gotten the press.

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

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

22 Mr. Latta. The chair now recognizes the gentleman from
23 Texas for 5 minutes.

24 Mr. Green. Thank you, Mr. Chairman, and I apologize. We
25 have a Health Subcommittee upstairs and I appreciate it. That

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 is not to take away the importance of this hearing. I want to
2 thank you and our ranking member for setting it.

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

18 When restaurants fail regular health inspections they are
19 routinely shut down for violations. They are shut down even if
20 problems aren't yet occurred as a consequence of their violations.
21 It isn't clear to me why Equifax, who is beyond that point, should
22 be allowed to continue operating when they have failed
23 spectacularly at their core business and endangered the public.
24 In the next couple months, Senate Republicans may repeal the
25 Consumer Financial Protection Bureau's arbitration rule thus

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 allowing companies like Equifax to put clauses in their fine print
2 forcing individuals into arbitration agreements instead of class
3 action agreements where they stand a chance of being able to cover
4 some of their loss.

5 But it should be clear to us by all that is now not the time
6 to roll back consumer safeguards in the financial industry and
7 I support my colleague and our ranking member Congresswoman
8 Schakowsky's Secure and Protect Americans' Data Act. I look
9 forward to hearing what our witness has to say. Mr. Smith,
10 ID theft protection companies have seen a big jump in business
11 and share price since the breach of your company including
12 LifeLock who has reported a tenfold increase in enrollment for
13 their credit monitoring and other services. LifeLock has a
14 contract to purchase credit monitoring services from Equifax,
15 meaning that every time someone signs up for LifeLock protection
16 from the impact of Equifax' data breach they are again
17 involuntarily sign up for Equifax to provide those services and
18 Equifax makes money on that breach. What is the value of that
19 contract that LifeLock has with Equifax?

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

23 Mr. Green. Okay. If it is available I would hope you would
24 send it and share it with the committee. Mr. Smith, an Equifax
25 report marketed to its business customers says that leading

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 lifestyle databases available commercially offer hundreds of
2 response segments covering almost every conceivable aspect of how
3 consumers live and what they spend their money on and what interest
4 they have.

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

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

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

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

24 Mr. Smith. If I understand the question, Congressman, we
25 take the data that is given to us by the credit ecosystem of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 U.S., add analytics to it, and then when a consumer wants credit
2 again through credit card, home loan, a car, the bank then comes
3 to us for that data and for that analytics and we charge them for
4 that.

5 Mr. Green. Okay. Well, the question was how many times
6 does Equifax receive payment for that individual credit file?
7 Every time -- if my local car dealer contacts Equifax and so they
8 pay a fee to Equifax for that information?

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

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

15 Mr. Green. I am sorry?

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

18 Mr. Green. Oh, okay. Oh, I thought I just had a perpetual
19 time.

20 Mr. Latta. No.

21 Mr. Green. Mr. Chairman, I just have one more question.
22 The products that Equifax are so far providing victims of the
23 breach do not include anything they won't need if it weren't for
24 Equifax's laxes on their data. You, however, made more than \$69
25 million in 2016. And so, but that is the concern that this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 committee has and I know we have for all our constituents.

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

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

6 Mr. Mullin. Thank you, Mr. Chairman.

7 Mr. Smith, what is your current job?

8 Mr. Smith. I am retired.

9 Mr. Mullin. You are retiring. Are you still getting paid
10 by the company?

11 Mr. Smith. No, sir.

12 Mr. Mullin. So you are fully retired and so you have no
13 affiliation at all with the company? You are not on as a
14 contractor or as --

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

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

25 Mr. Smith. Nothing. The day I announced my retirement that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 ended.

2 Mr. Mullin. Do you still own stock in the company?

3 Mr. Smith. I am sorry?

4 Mr. Mullin. Do you still have stock in the company?

5 Mr. Smith. Oh, yes.

6 Mr. Mullin. Have you sold any of it?

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

8 Mr. Mullin. In recent, since this has become aware to the
9 public?

10 Mr. Smith. During this breach?

11 Mr. Mullin. Yes.

12 Mr. Smith. Oh. No, sir.

13 Mr. Mullin. Are you aware of the individuals that have?

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

16 Mr. Mullin. That sold stock?

17 Mr. Smith. Yes. One -- yes, and all three of them are men
18 I have known, I mentioned earlier, for a number of years. Two
19 for almost 12 years and one for 3 or 4 years and they are men of
20 high integrity.

21 Mr. Mullin. Did they sell it before this went public?

22 Mr. Smith. Yes. As I said before, the knowledge -- we went
23 public with this on September 7th.

24 Mr. Mullin. And when did they sell their stock?

25 Mr. Smith. August 1st and 2nd.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Mullin. So after the breach?

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

6 Mr. Mullin. So what would cause them to sell it?

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

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

15 Mr. Smith. If I can clarify?

16 Mr. Mullin. Yes.

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

20 Mr. Mullin. Right.

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

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

25 Mr. Smith. Ultimately me.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 Mr. Smith. There was on the vulnerability side, there was
4 the --

5 Mr. Mullin. Do you have a department that is dedicated to
6 this?

7 Mr. Smith. Yes. There is a chief information officer who
8 was ultimately responsible. He was --

9 Mr. Mullin. Is that person still over that department?

10 Mr. Smith. No, sir. He is gone.

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

14 Mr. Smith. Notification.

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

22 These four things that you named were common sense, things
23 that should have been put in place to begin with. It should have
24 been the fire alarm. You are in that world. This should be on
25 the side of the wall where you pull the handle and it immediately

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 goes into place. How was it that it was just now thought of that
2 you needed to have four common sense principles put in place on
3 how to react to something in a world where we knew you were
4 vulnerable at?

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

10 The one thing, Congressman, it is not a switch on a wall.
11 It is the ability to stand up the environment we had to stand up
12 --

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

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

25 Mrs. Walters. Thank you, Mr. Chairman.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

8 Now Equifax's business model depends on gathering consumer
9 information, repackaging it, and selling it. Equifax has set up
10 a website in which consumers can enter information to determine
11 if they are at risk and sign up for credit monitoring and credit
12 lock. To participate, a person has to give Equifax the same type
13 of personal information, including Social Security Number, which
14 Equifax put at risk in this breach. I want to know what Equifax
15 is planning to do with this information besides offering credit
16 monitoring and credit locks. Can you ensure me that Equifax will
17 not plug this information back into its core business operation
18 and sell it to its lenders?

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

22 Mr. Smith. Congresswoman, thank you for your comments.
23 And as I mentioned in my written testimony and my oral testimony,
24 I have said throughout the morning and I will say again today,
25 as the CEO it was under my watch. I am responsible. I am

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 accountable and I apologize to all of your consumers in
2 California.

3 The intent of this offering that we are giving to your
4 constituents in California and to consumers across the country
5 is in an environment where we are not going to sell other products.
6 It is to come there and be service protection of the five offerings
7 that you had mentioned, not to sell and take your data and monetize
8 that. It is to take and protect you with these five services.

9 Mrs. Walters. Equifax's breach notification website uses
10 a stock installation of WordPress. This causes me a lot of
11 concern because it seems to have insufficient security for a site
12 asking people to provide part of their Social Security Number.
13 Can you assure me that this website is secure and will not further
14 endanger the personal information of my constituents?

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

24 Mrs. Walters. Okay. And finally, my last question is how
25 many U.S. consumers have enrolled in the credit monitoring service

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 TrustedID? I will just finish here, because I know multiple
2 people who have enrolled including my immediate family and they
3 were told that they would receive an email to complete the process.
4 After days of waiting they have not received an email and wanted
5 to know what the delay in processing this protection and when will
6 they be able to complete the process to help protect their
7 information?

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

17 Mrs. Walters. Okay, thank you. And I yield back the
18 balance of my time.

19 Mr. Latta. Thank you very much. The gentlelady yields back
20 and the chair now recognizes the gentleman from Pennsylvania for
21 5 minutes.

22 Mr. Costello. Thank you, Mr. Chairman. I have heard from
23 hundreds of constituents in my congressional district. There are
24 approximately five and a half million in Pennsylvania. I have
25 reviewed each and every one of the constituent stories that I have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 received.

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

9 And it is this last one that is so particularly angering
10 because it is going to potentially be so destructive to hundreds
11 of millions of Americans what might happen to them in the years
12 to come. And as the head of the company and throughout the
13 company, the culture of that company has to know how predictable
14 the damage can potentially be.

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

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

24 Mr. Costello. See, I think the anger is going to be
25 multiplied thousands of times when something actually happens.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 So when you talk about how predictable some of this is, the rollout
2 of the call centers and the second rollout and the third rollout,
3 it has to be predictable how massive this is and what would need
4 to be put in place from a protocol perspective in order to address
5 what is coming.

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

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

17 Mr. Costello. I understand, the hurricane.

18 Mr. Smith. -- taken out by Hurricane Irma. We were not
19 prepared for that kind of call volume.

20 Mr. Costello. How couldn't you be? How couldn't you be?

21 Mr. Smith. It is not our traditional business model. Our
22 traditional business model is dealing with companies, not 400
23 million consumers coming to the website.

24 Mr. Costello. But your business model has a couple hundred
25 million customers, so on a breach of this scale obviously you are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 going to have at least that number and probably twice that amount
2 calling, inquiring as to whether or not they are subject to the
3 breach and that wasn't done.

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

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

13 Mr. Smith. Yes.

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

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

21 Mr. Costello. How would you know that you are in compliance
22 then? Because if you said you followed protocol and protocol led
23 to this, then it is very difficult for me -- I mean that calls
24 into question whether the Safeguards Rule is sufficient enough.
25 Because if you are saying you are in compliance with it and you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 followed protocol and this still happened that unearths a whole
2 other set of questions.

3 Mr. Smith. Again the speed of reaction and the scale of the
4 reaction was unprecedented for -- I am not taking any excuses.

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

13 And it just seems to me that through insurance policies,
14 through reporting to your board, through your board wanting to
15 make sure that they are doing their job that you are going to be
16 looking for certifications from your outside forensic consultants
17 doing audits to say yes, you are doing good. You are doing good.
18 Here are the new threats. Here is how we are updating. And I
19 just don't see -- that is the kind of information I think would
20 be extremely helpful that we have not received any information
21 from today.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 complied with protocol. When was the last time that was updated?

2 Mr. Smith. I understand your question. We will get you
3 that information.

4 Mr. Costello. Do you yield back after you are already well
5 over? I yield back.

6 Mr. Latta. Your time is expired, how is that? The chair
7 now recognizes the gentleman from Georgia -- I am sorry. I am
8 sorry. The gentleman from New York, 5 minutes.

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

16 Mr. Smith, we are here today because months after the breach
17 actually took place your company, Equifax, revealed that its
18 for-profit business practices have exposed the highly sensitive
19 personal information of some 145-1/2 million Americans and
20 counting. Your data breach exposed a critical vulnerability in
21 the American economy and the information security of the American
22 people. Victims of this breach span every age group, every race,
23 class, and other demographic. They now face a lifetime at risk
24 of fraud, identity theft, and other crimes as a result of the
25 private data that you exposed.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

19 Mr. Smith. You know, a crisis that never occurs if
20 everything has gone right. In this case as I mentioned earlier
21 we had a human error and a technology error. It wasn't because
22 we were unwilling or unable to make the financial investments in
23 people, process, or technology though.

24 Mr. Tonko. My constituent Tanya asks, how do I get Equifax
25 to fix this without signing over my rights and what related costs

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 will I, Tanya, be expected to pay over my lifetime?

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

8 Mr. Tonko. And any related costs that she should expect to
9 pay over her --

10 Mr. Smith. Those services are all free.

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

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

21 Mr. Tonko. Constituent Lee (ph.) from Albany asks, why are
22 you using this gross misconduct to turn your victims into
23 customers for a paid monitoring service that you will profit from?

24 Mr. Smith. That is not the intent. Our intent is to offer
25 those five services for free followed by the sixth service which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 is a lifetime lock for free.

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

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

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

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

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

23 Mr. Smith. At this point all indication are it was at
24 random. It was not targeting of individuals specifically.

25 Mr. Tonko. I have exhausted my time, but let me assure you,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Smith, I have many, many, many constituent questions that
2 continue to pour forth and we are going to provide those after
3 the hearing here and would expect that they would all be answered.
4 And again thank you for your response. I yield back, Mr. Chair.

5 Mr. Latta. Thank you very much. The gentleman yields back
6 and the chair now recognizes the gentleman from Pennsylvania for
7 5 minutes.

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

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

20 Mr. Smith. I have no knowledge of that. I have no knowledge
21 of that being the case.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Mr. Smith. Could you repeat the question, please?

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

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

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

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

14 Mr. Murphy. We have also heard a lot about the website
15 Equifax set up to handle the consumer protection response at
16 equifaxsecurity2017.com. As it has been pointed out, this looks
17 like a website that scanners would use for phishing. In fact,
18 it was widely reported in the press someone switched two words
19 and made it into phishing website that looked almost identical.
20 Luckily, this person was just trying to make a point, but I think
21 that point is well taken.

22 You said earlier today that you set up this external website
23 because Equifax's own domain wouldn't be able to handle the sheer
24 amount of traffic. Now why wouldn't your website be able to
25 handle this traffic? I mean it just doesn't make sense a company

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 of your size and knowledge doesn't understand how to handle
2 traffic for over a 100 million people. Don't you use an elastic
3 cloud computing service that would have accounted for this
4 traffic?

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

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

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

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

23 Our understanding is that fixing this vulnerability required
24 more effort than simply installing a patch. But we also
25 understand that when Equifax did patch the vulnerability it took

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 less than 3 days to do so. So if the patch only took a few days
2 to apply, why did Equifax fail to install it immediately after
3 it was announced as critical?

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

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

11 Mr. Smith. I know of no standard protocol that we would
12 notify --

13 Mr. Murphy. I didn't ask about standard protocol. I asked
14 did you notify people.

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

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

20 Mr. Smith. I have no knowledge of need --

21 Mr. Murphy. Did you notify other people -- did other people
22 and the executives of your company, were you aware of it?

23 Mr. Smith. As I have said before I was not.

24 Mr. Murphy. You were not aware that there was this problem
25 with the vulnerability? You just told me it takes a few days or

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 a few weeks, but you weren't aware that it existed?

2 Mr. Smith. That is correct.

3 Mr. Murphy. Well, let me wrap up with one final thought
4 here. In your testimony you state that the breach occurred
5 because of both human error and technological failures, or
6 technology failures. So looking at the three features I just
7 highlighted -- the improperly configured scans, the poorly chosen
8 website, the lack of patching -- these are not failures of
9 technology. A human misconfigured the scan. A human selected
10 the website name. A human failed to apply the patch.

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

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

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

24 Mr. Sarbanes. Thank you, Mr. Chairman.

25 Mr. Smith, thank you for being here. You have been the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 president of the company for, CEO for 12 years; is that right?

2 Mr. Smith. That is correct.

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

7 First of all, they want to understand. And you have tried
8 to explain it today, but I am not sure it is going to be
9 satisfactory why there wasn't sufficient protections in place on
10 the front end so that this kind of breach wouldn't happen in the
11 first place given the sensitivity of the information that you are
12 keeping in the company. The second thing is how quickly once a
13 breach was discovered you came clean to the public and provided
14 information on what was happening. There seems to have been a
15 delay there that concerns people.

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

24 I wanted to ask you about the kind of remedies that you have
25 out there because there is some confusion. I got a question from

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 a constituent who had purchased a monitoring service that would
2 cover his family including a child under the age of 18. So first
3 of all, can you tell me, it is possible for someone under the age
4 of 18 to have their identity stolen; is that correct as far as
5 you understand?

6 Mr. Smith. Is it possible?

7 Mr. Sarbanes. Yes.

8 Mr. Smith. As it relates to this breach?

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

12 Mr. Smith. If someone has a Social Security Number, at any
13 age, can that be compromised, yes. It could not be compromised
14 in this case because this database they got into it is my
15 understanding only was for those who had credit, credit active
16 or inactive, and they have been in a credit environment.

17 Mr. Sarbanes. Okay. But my understanding is that when you
18 provide a family service you are collecting information and
19 holding information that includes the Social Security Number of
20 people who may be under the age of 18.

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

23 Mr. Sarbanes. Okay.

24 Mr. Smith. But I have no knowledge.

25 Mr. Sarbanes. If that is the case, is this free service that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 you are providing going to cover any exposure or information that
2 is related to a minor, as opposed to somebody who is over the age
3 of 18, if you had information on that minor?

4 Mr. Smith. I can look into that Congressman. The intent
5 of the coverage was to cover anyone in America who is in the credit
6 system. So if you are under 18 and not in the credit system, I
7 will check your one point which is on this concept called family
8 plan that you are alluding to where you lock down consumers, you
9 monitor consumers. I don't believe their Social Security Numbers
10 were in this system, but we can verify that.

11 Mr. Sarbanes. Well, that is important because --

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

14 Mr. Sarbanes. Okay. I think it is important because it may
15 be that with respect to credit reporting the implications of this
16 breach only attach to people that are 18 or older. But if you
17 are holding information about minors like a Social Security Number
18 that is part of the portfolio of information you are getting from
19 a family, for example, particularly when the family has paid for
20 this service, you are holding their Social Security Number, so
21 any breach that makes that information available outside of the
22 arena in which it is supposed to be kept close creates
23 vulnerability for that person.

24 It is not like we get a new Social Security Number when we
25 turn 18. So that is going to follow them all the way through and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 create some real risk for them. So I think that is a piece of
2 this that we need to understand much better, and I want to thank
3 my constituents for sort of bringing that to our attention.

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

7 Mr. Sarbanes. Thank you. I yield back.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 has ever happened, but it has happened to other companies before.

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

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

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

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

24 Mr. Carter. Let me ask you this. Through this scenario,
25 through this experience, rather, if you had to do anything

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 different what would you have done?

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

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

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

23 Mr. Carter. And I understand that and I appreciate that.

24 Mr. Smith. If there is one thing I would love to see this
25 country think about is, the concept of a Social Security Number

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 in this environment being private and secure, I think it is time
2 as a country to think beyond that. What is a better way to
3 identify consumers in our country in a very secure way, and I think
4 that way is something different than an SSN, a date of birth, and
5 a name.

6 Mr. Carter. Well, you are exactly right. I remember my
7 time in the Georgia State Legislature when we changed the, you
8 know, you used to have your Social Security Number on your driver's
9 license. That used to be your driver's license number, you know,
10 and we changed -- and that was not that long ago. And that is
11 what tells me that this is something that is changing dramatically
12 and quickly and we need to be prepared for it.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 you, Mr. Chairman. I yield back.

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

4 Ms. Eshoo. Thank you, Mr. Chairman. First, I would like
5 to recognize a former colleague that is here in the chamber with
6 us. Saxby Chambliss who served in the House and in the Senate,
7 it is good to see you, very nice to see you.

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

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

23 Now it has been, the question has kind of been posed
24 rhetorically by some members, because I have been sitting in for
25 awhile at this hearing, what can be done. I have the privilege

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 of representing most of Silicon Valley. I have asked this
2 question about the protection in terms of privacy breaches in our
3 country to just about every CEO I have met and they have responded
4 like a chorus and said there are two main reasons for breaches
5 in our country, number one, a lack of hygiene in systems and very
6 poor security management. That is why I have legislation.
7 Senator Hatch is the lead sponsor in the Senate. I have the bill
8 in the House.

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

19 Mr. Smith. Congresswoman, to clarify, when the CERT came
20 out in March there was no notification of a breach. There was
21 notification --

22 Ms. Eshoo. What did it mean?

23 Mr. Smith. What it meant was --

24 Ms. Eshoo. I mean if I got a notice from Homeland Security
25 that is like the FBI knocking on the door. I mean it is the federal

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 government. That in and of itself is a bit menacing, isn't it?

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

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

7 Mr. Smith. We get notifications --

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

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

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

17 Mr. Smith. The security team did and they spoke with the
18 IT team as well.

19 Ms. Eshoo. When did they take care of it?

20 Mr. Smith. Throughout the testimony we talked about what
21 occurred was there was a communicate --

22 Ms. Eshoo. Well, just tell me when it happened. When was
23 it actually --

24 Mr. Smith. The following day communication was sent out to
25 those that needed to be notified.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

16 Nice to see you, Saxby.

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

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

24 Mr. Latta. Without objection, so ordered.

25 [The information follows:]

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1

2

*****COMMITTEE INSERT 2*****

1 Ms. Schakowsky. Oh, sorry.

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

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

16 Ms. Schakowsky. No, I understand that and that is exactly
17 where we need to go, to a much larger discussion because most
18 Americans really don't know how much information, what it is, that
19 you have it, and they never said okay. So I am hoping this will
20 lead to a wider discussion. Thank you.

21 Mr. Latta. Thank you very much. The gentlelady yields
22 back. And if I may just to go back to what we had a little
23 discussion earlier, again going back to your testimony. From
24 August the 15th when you were informed that it appeared likely
25 that consumer, that information had been stolen, again why was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 there again a 10-day delay between finding out about that personal
2 information that could have likely been stolen to developing that
3 remediation plan? That 10-day window, why did it take 10 days
4 to start that remediation?

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

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

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

25 Mr. Latta. Well, thank you very much. And seeing that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 there are no other members present to ask questions, we want to
2 thank you very much for testifying before the subcommittee today.
3 And pursuant to committee rules I remind members that they have
4 10 business days to submit additional questions for the record
5 and I ask that the witness submit his response within 10 business
6 days upon request of any questions submitted. Without objection,
7 the subcommittee is adjourned.

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