EQUIFAX RESPONSE SUBMITTED JANUARY 26, 2018

Written Questions for the Record from the Honorable Robert E. Latta

1. In your testimony, you stated "at my direction a well-known, independent expert consulting firm (in addition to and different from Mandiant) has been retained to perform a top-to-bottom assessment of the company's information security systems."

a. What is the name of this cybersecurity firm?

b. When was this firm engaged by Equifax to provide this security assessment?

c. What is the specific scope of work relating to the assessment of the company's information security systems that Equifax requested to be completed by the firm?

d. Why did Equifax engage this firm if Mandiant was already under contract with Equifax?

Response: Equifax engaged PwC on September 22, 2017 to assist with its security program, including strategic remediation and transformation initiatives that will help the Company identify and implement solutions to strengthen its long-term data protection and cybersecurity posture. The engagement with PwC is different from the scope of Mandiant's engagement. Mandiant reviewed forensic, network, and log data from Equifax to determine: (1) the earliest date of compromise and method of intrusion; (2) the scope of the intrusion; (3) whether the intrusion was ongoing; and (4) the extent of data exposure and exfiltration. Mandiant also performed containment and remediation-related planning, and monitored network traffic for the affected web application environment for any ongoing attacks.

2. According to a Bloomberg Businessweek investigation, allegedly "Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, a person familiar with the perspectives of both sides said."

a. Did Mandiant, in fact, convey these warnings to Equifax management, and did company officials agree with the Mandiant assessment?

b. When did Mandiant first issue to you or Equifax senior management warnings that unpatched systems could indicate major data breach and data theft problems?

c. Please detail each time in 2017 that Mandiant issued such warnings to you or the company.

d. If Equifax disagreed with Mandiant on the security assessment or for any other reason, did any disagreement materially affect the time to address the breach and to initiate the breach notification and consumer protection remediation?

e. What impact did any disagreement with Mandiant have on engaging the new, well-known cybersecurity firm you noted in your written testimony?

Response: The Bloomberg story published on September 29, 2017 inaccurately conflates two separate, unrelated cybersecurity events.

The events described in the article appear to inaccurately reference fraud incidents experienced by TALX Corporation, a wholly-owned subsidiary of Equifax. TALX Corporation, operating under the trade name Equifax Workforce Solutions, provides human resources, payroll, tax management, and compliance services. These fraud incidents were not related to the recent cybersecurity incident (see, in pertinent part, Mandiant's supplemental report, produced today as an attachment to this response). A brief background summary of these fraud incidents follows:

- TALX experienced fraud incidents during the spring of 2016 and the spring of 2017.

- During the spring of 2016, fraudsters used personal information obtained from non-Equifax sources to access employee accounts that used personally identifiable information for the user ID and personal information for the related default PIN. In response to the 2016 unauthorized access, TALX added an additional layer of authentication for the 2017 tax season.

- During the spring of 2017, TALX received reports of unauthorized access to individuals' W-2 tax forms contained within TALX's online platform. This incident did not involve any hacking of Equifax systems, and there was no mass exfiltration of data.

- Mandiant was hired to assist with the TALX fraud investigation. The situation was also reported to law enforcement. Mandiant investigated both events and found no

evidence that the fraud incidents involving TALX were related to the cybersecurity incident announced on September 7, 2017.

3. According to a Bloomberg Businessweek investigation, reportedly "there [were] signs that Smith and others were aware something far more serious was going on. The investigation in March was described internally as 'a top-secret project' and one that Smith was overseeing personally." According to your testimony, the early March timeframe was when the U.S. Computer Emergency Readiness Team dispatched its notice on the Apache Struts vulnerability.

a. Please describe this "top-secret project" or any other direct discussions you were a part of regarding Equifax's cybersecurity practices or vulnerabilities from January 2017 to July 29, 2017.

Response: Please see response to Question 2.

4. In your testimony you noted "the breach occurred because of both human error and technology failures. These mistakes—made in the same chain of security systems designed with redundancies."

a. What was the specific process for reporting cybersecurity vulnerability issues and data breaches up to the CEO's office, other senior executives, and the board of directors from January 20l7 to July 29, 2017?

b. What was the specific process for reporting cybersecurity vulnerability issues and data breaches up to the CEO's office, other senior executives, and the board of directors after July 29, 2017?

Response: From January to July 29, 2017, Equifax had a formalized security program supported by administrative, technical, and physical safeguards focused on the protection of consumer data. Equifax had a security team in place, which was responsible for the coordination and execution of the Company's information security program. The security team reported to Equifax's Chief Security Officer ("CSO") and operated using defined plans and procedures for responding to security incidents, which were revised on a regular basis. The CSO then determined whether and when any particular cybersecurity incident should be reported to others including the Chief Legal Officer (to whom the CSO reported at the time), the CEO's office, other senior executives, and the board of directors. This responsibility remained with the CSO after July 29, 2017, but the CSO now reports directly to the CEO rather than to the Chief Legal Officer.

4. In your testimony you noted "the breach occurred because of both human error and technology failures. These mistakes – made in the same chain of security systems designed with redundancies."

a. What was the specific process for reporting cybersecurity vulnerability issues and data breaches up to the CEO's office, other senior executives, and the board of directors from January 20l7 to July 29, 2017?

b. What was the specific process for reporting cybersecurity vulnerability issues and data breaches up to the CEO's office, other senior executives, and the board of directors after July 29, 2017?

Response: From January 2017 to July 29, 2017, Equifax had a formalized security program supported by administrative, technical, and physical safeguards focused on the protection of consumer data. Equifax had a security team in place, which was responsible for the coordination and execution of the Company's information security program. The security team reported to Equifax's Chief Security Officer ("CSO") and operated using defined plans and procedures for responding to security incidents, which were revised on a regular basis. The CSO then determined whether and when any particular cybersecurity incident should be reported up to the Chief Legal Officer (to whom the CSO reported at the time), who then determined what was reported to the CEO's office, other senior executives, and the board of directors. This responsibility remained with the CSO after July 29, 2017, but the CSO now reports directly to the CEO rather than to the Chief Legal Officer.

c. How many reports about unauthorized access into Equifax's system did you receive as CEO?

Response: As Mr. Smith testified, Equifax experiences millions of suspicious activity threats against its systems every year, which are, from time-to-time, escalated to the CEO pursuant to the company's cybersecurity policies and procedures. Given this volume, there is no way for Mr. Smith to quantify the number of reports of such suspicious activity or attacks he may have received during his twelve years as CEO. However, to the best of his knowledge, Mr. Smith believes Equifax's security team followed all applicable plans and procedures for responding to cybersecurity incidents, including with respect to reporting and elevating cybersecurity incidents to appropriate executives within the company and the board of directors.

d. What was the standard used by your direct reports to determine when an event qualified to tell you about the unauthorized access?

Response: As stated in response to Question 4a-b, Equifax operated using defined plans and procedures for responding to security incidents. Equifax's plans and policies to address cybersecurity incidents included its Security Incident Handling Procedure Guide (the "Incident Guide") and its predecessor guides, which have been in place since at least 2008. Equifax's Security Incident Response Team Plan ("SIRT Plan") and its predecessor plans have been in place since at least 2013. These guides and plans have been updated and refined over time, including changes to the titles of the operative documents. Copies of the plans were provided with our January 26, 2018 submission and Bates-numbered EFXCONG-EC000000552 to EFXCONG-EC000000605 (*See* Response to Congressman Mullin's Question 1).

As set forth in response to 4 a-b, the security team reported to Equifax's CSO, who then determined whether and when any particular cybersecurity incident should be reported up to the Chief Legal Officer (to whom the CSO reported at the time), who then determined what was reported to the CEO's office, other senior executives, and the board of directors.

5. Please describe the resources, investments and operating expenditures that Equifax had focused on its information security prior to July 2017 for the three preceding years.

a. What percentage of Equifax's balance sheet for the last three years was put into maintaining and upgrading the company's global IT security systems?

Response: Security experts recommend—and the industry has generally adopted as standard—an expenditure of 10–14% of IT budget on security. Equifax has spent within that range for the last three years. Since the breach, Equifax has spent considerably above that standard to harden security.

6. Prior to the breach, who did the former Chief Security Officer at Equifax report to? How many full-time employees were employed in the Information Security office?

a. After the breach, who does the Chief Security Officer at Equifax report to? How many full-time employees are now employed in the Information Security office?

Response: Prior to her retirement, the former Chief Security Officer at Equifax reported to the Chief Legal Officer. The interim Chief Security Officer at Equifax currently reports directly to the interim CEO. As of June 30, 2017, the end of the quarter prior to Equifax discovering the cybersecurity incident, there were approximately 232 full-time employees in the Security department. As of December 1, 2017, there were approximately 239 full-time employees in the Security department. In addition to full-time employees, the Security department also engages third parties to assist with information security efforts.

7. Prior to the breach, who did the former Chief Information Officer at Equifax report to? How many full-time employees were employed in the Information Technology office?

a. After the breach, who does the Chief Information Officer at Equifax report to? How many full-time employees are now employed in the Information Technology office?

Response: Prior to his retirement, the Chief Information Officer reported to the Chief Executive Officer. The interim Chief Information Officer reports to the interim Chief Executive Officer. As of June 30, 2017, the end of the quarter prior to Equifax discovering the cybersecurity incident, there were approximately 2,497 full-time employees employed in the Information Technology department. As of December 1, 2017, there were approximately 2,600 full-time employees employed in the Information Technology office.

8. What percentage of Equifax's balance sheet for the last three years was put into hiring, training and retention of security and/or information technology (application owner) employees? What is the percentage following the breach?

Response: Security experts recommend—and the industry has generally adopted as standard—an expenditure of 10–14% of IT budget on security. Equifax has spent within that range for the last three years. Since the breach, Equifax has spent considerably above that standard to strengthen security. Equifax expects that increase in spending to continue for a period of time.

9. In your testimony you mentioned "suspicious activity" numerous times, and seemed to distinguish "suspicious activity" with a breach incident. Is there a meaningful difference between suspicious activity and a breach in how events are reported up the security and information technology departments at Equifax during your tenure? Please describe the differences and if any different terminology was used internally to describe events where unauthorized actors gained access to the Equifax system and/or removed data (personal or otherwise) from the Equifax system.

Response: "Suspicious activity" typically refers to electronic activity or transactions that appear to be anomalous or potentially inconsistent with normal electronic activity. Suspicious activity does not necessarily indicate a breach. "Breach" typically refers to a verified, unauthorized intrusion into a network. A breach may, but does not necessarily, include exfiltration of data.

Equifax's Security Incident Response Standard in place in July 2017 requires, among other things, that employees report as soon as practical to their manager or to the Company's Cyber Threat Center all known or suspected security vulnerabilities, weaknesses, violations and unauthorized disclosure of information classified as Confidential or higher. If reported to a manager, the manager must escalate any reported issue to a member of the Company's Security team as quickly as possible. Known or suspected security breaches must be reported in the same manner regardless of location of the breach, including within the Company or within a third party holding the Company's information. If the security event or incident involves a user's immediate manager, the user may report the incident to his or her manager's next level of supervision, another manager, the Company's Cyber Threat Center, or to the Chief Security Officer.

The Security Incident Response Standard defines a "Security Incident" as the violation of an explicit security requirement resulting in the interruption of or interference with any part of the business, including processes, services and systems. The Security Incident Response Standard provides several examples of types of Security Incidents, including system failures, phishing emails, sending information inappropriately through email, denial of service attacks, unauthorized or improper access of information, physical damage to company assets, theft, loss, property damage, bomb threats, and natural and man-made disasters.

A copy of the Security Incident Response Standard has been provided with this submission and Bates-numbered EFXCONG-EC000002449 to EFXCONG-EC000002454 on the enclosed CD, which has been encrypted. The password to gain access to the documents will be sent by separate correspondence.

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

Response: As of January 23, 2018, approximately 11.09 million consumers had completed registration for TrustedID Premier and approximately 4.16 million consumers completed the enrollment process.

Written Questions for the Record from the Honorable Brett Guthrie

1. Thank you for testifying before our Subcommittee. My question relates to concerns I've received from constituents attempting to sign up for the credit freeze or free credit monitoring features through your website and phone hotline.

The primary concern is that when consumers attempt to sign up online they are having trouble navigating to the form page required to file their requests. Some consumers are nervous about submitting their information online, but they are also finding it difficult to navigate the telephone menu options, sometimes even finding the choices circuitous.

a. Are you aware of these issues that my constituents have raised regarding the challenges of the telephone and on line processes?

b. What specific steps are you taking to simplify the online forms and telephone hotline to make a more direct connection to the required forms and call center professionals, ensuring that consumers are able to take advantage of the services you are offering?

Response: Website: Equifax is continuously working to enhance and improve consumers' experience with the incident website, www.equifaxsecurity2017.com. The Company created more intuitive navigation on the microsite and reduced the number of phone numbers listed. Following the initial launch of the "Am I impacted?" search tool on September 7, 2017, the Company resolved some technical issues with the search functionality. Following the completion of a forensic investigation on October 2, 2017, the Company is now able to provide a more definite impact response to U.S. consumers who take advantage of the "Am I impacted?" search tool, which can be accessed by going to the home page of the site.

In addition, following completion of the forensic investigation on October 2, 2017, the Company has (1) mailed written notices to the approximately 2.5 million additional U.S. consumers that were potentially impacted; and (2) updated the "Am I impacted?" search tool on the website to include the entire impacted population of approximately 145.5 million U.S. consumers.

Call Centers: Since the incident was announced, Equifax also has scaled up its call center operations to ensure it has more than enough associates to handle calls from concerned consumers.

Equifax added several new types of call centers to the original breach response call center that was launched on September 7, 2017. New call centers included a Breach Response Call Center to handle frequently asked questions about the incident, a call center for TrustedID Premier Authentication and Enrollment Assistance, and a TrustedID Premier Support Call Center. The call centers are open seven days a week from 7am–1am Eastern. Approximately 3,400 additional call center agents were added to the 770 original agents, and all of the agents

received extensive, incident-specific training. This additional staffing reduced the average wait time from 10-30 minutes to less than one minute.

Equifax has continued to make enhancements to the call centers, such as: providing additional training and ongoing updates for agents; adding staff to oversee call center processes; conducting regular and ongoing calls with vendors to discuss agent issues and IT issues; having company leadership visit call centers; conducting agent focus groups; and adding call back functionality to the process.

Written Questions for the Record from the Honorable David B. McKinley

1. So far, 730,000 West Virginians were affected by the breach. That's nearly 40 percent of our population. With so many people affected, communication with law enforcement and other bodies is important, from the federal level all the way down to the local level.

a. When did Equifax alert federal law enforcement and other authorities to the data breach?

b. Can you please specify what Federal and regulatory authorities were alerted, when, and what action each organization suggested or required?

c. At what point did the company alert State law enforcement and other authorities to the data breach?

d. Did Equifax inform any of its State regulators of the breach before informing the public?

Response: Equifax notified the Federal Bureau of Investigation about the suspicious activity on August 2, 2017. Equifax notified the Federal Trade Commission and the Consumer Financial Protection Bureau of the cybersecurity incident via phone calls on September 7, 2017, at approximately the same time Equifax published its official press release. Equifax also provided written notifications to 52 state attorneys general on September 7, 2017.

Upon the completion of the forensic investigation, Equifax also provided supplemental notifications to those 52 state attorneys general on October 12, 2017.

Equifax continues to cooperate with regulators, federal agencies, legislators, and law enforcement agencies in connection with the cybersecurity incident, and the company expects to continue to do so in the future.

2. Why weren't the states notified earlier so they could better prepare a plan to inform their residents and set up additional resources for concerned consumers?

Response: Please see responses to Question 1. Equifax complied with all state data breach notification requirements, including the requirement in many state data breach statutes that notification to state attorneys general and other state regulators be made at the time of notification to the potentially impacted consumers.

3. How have you assisted state and local bodies in their efforts to inform their residents?

Response: Equifax provided written notifications to 52 state attorneys general on September 7, 2017. Upon the completion of the forensic investigation, Equifax also provided supplemental notifications to those 52 state attorneys general on October 12, 2017. Equifax continues to cooperate with the state attorneys general in connection with the cybersecurity incident.

4. Do you think you could be doing more to inform potentially affected consumers?

Response: Equifax has continually improved its support for consumers. The company has scaled up its call centers to answer consumer calls more promptly. Equifax also has made a series of improvements to its incident website to make it more user friendly, and has created a Spanish language website. In addition, Equifax is listening to consumers through an expanded social media effort.

Equifax also supports a single federal breach notification standard. At the request of the Senate Commerce Committee, Equifax has provided its recommendations on that issue. A single federal breach notification standard would help ensure that all impacted consumers and regulators receive the same information regarding a breach incident in an efficient and expedient manner. Lawmakers may want to consider key elements in developing a federal standard including:

- **Direct and Substitute Notices**: All state statutes provide for a substitute or alternate notice versus a direct notice to consumers depending on the cost of a direct notice, the universe of affected consumers residing in the state, or the lack of sufficient contact information for the consumers. States agree that flexibility is important when considering notification, and that all breach incidents should not necessarily require a direct notification to all impacted consumers.

- **Timing**: Many states require notification "in the most expedient time and manner possible and without unreasonable delay" following the discovery of a breach (for example, New York and California data breach statutes). This standard allows the breached entity time to determine the scope of the incident and the number of consumers impacted, and to restore the integrity of systems before moving forward with public notification. While a minority of states require notice within a specific time frame, generally between 30 to 45 days, most states recognize that it is important for a breached entity to conduct an investigation and to complete corrective actions before providing notification. This will help ensure that the security or technological issue has been addressed and the breach notification is provided to the correct consumers and includes the most accurate information regarding the incident.

- **Content Notification**: Most states have the same general content requirements that include information such as: the date of the breach; a general description of the incident; the type of personally identifiable information ("PII") impacted; contact information for the breached entity; contact information for the consumer reporting agencies, the Federal Trade Commission, and Attorneys General; steps taken to prevent a further breach; and advice to consumers regarding protecting against identity theft. Some states, however, have state-specific requirements that require separate notification letters, as noted in the response above. Consistent content notification requirements across all states would ensure that consumers

receive the same information regarding a breach incident regardless of where they reside, and in an efficient manner.

- **Regulator Notices & Enforcement**: Some states require notice be provided to the state's Attorney General or other state regulators. A federal breach law may want to consider consolidating regulator notices to a single federal authority to streamline the initial notification, centralize follow-up requests and information regarding the incident, coordinate communication among various stakeholders, and, ultimately, enforce a federal breach notification standard.

Other provisions to consider when evaluating a federal breach notification standard should include: whether PII is "acquired" or "accessed" and how that determination relates to notification; whether the breached entity is a "data owner" versus a "maintainer;" the definition of PII; a risk-of-harm analysis when considering whether notification obligations are triggered; and how notification obligations are impacted by encryption of data and compromises of "electronic" versus "paper records."

Written Questions for the Record from the Honorable Markwayne Mullin

1. Did Equifax have a breach response plan in place before the event that outlined steps the company should take to protect consumers in the event of a data breach?

Response: Equifax has plans to address cybersecurity incidents, including but not limited to its "Security Incident Handling Procedure Guide" and its predecessor guides, which have been in place since at least 2008. Equifax's "Security Incident Response Team Plan" and its predecessor plans have been in place since at least 2013. These guides and plans have been updated and refined over time, including changes to the titles of the operative documents. Copies of these plans have been provided with this submission and Bates-numbered EFXCONG-EC000000552 to EFXCONG-EC000000605 on the enclosed CD, which has been encrypted. The password to gain access to the documents will be sent by separate correspondence. For the July 2017 Security Incident Handling Procedure Guide, please note that the document is stamped 'Draft.' Equifax understands that the content of this document was approved for use in August 2017, and are therefore providing it to you in its form at that time. The company further understands that the content of the June 2017 Security Incident Response Team Plan was also approved in August 2017.

2. If there was a response plan, did it include immediately notifying customers if their private information was revealed? What other protections or actions are captured in the breach plan?

Response: Please see the response to Question 1 and the crisis management documentation provided to the Subcommittee.

3. I had several constituents contact my office very frustrated after having spent hours on the phone unable to connect with Equifax customer service. Why were consumers unable to reach anyone by phone?

Response: The scale of this incident was enormous, and Equifax struggled with the initial volume of consumers utilizing its website and call centers. Since the initial rollout, Equifax has continually improved its support for consumers. Soon after the incident was announced, the company scaled up its call centers to answer consumer calls more promptly and to ensure that there are more than enough associates to handle calls from concerned consumers. Equifax added several new types of call centers to the original breach response call center that was launched on September 7, 2017. New call centers included a Breach Response Call Center to handle frequently asked questions about the incident, a call center for TrustedID Premier Authentication and Enrollment Assistance, and a TrustedID Premier Support Call Center. The call centers are open seven days a week from 7am–1am Eastern. Approximately 3,400 additional call center agents were added to the 770 original agents, and all of the agents received extensive, incident-specific training. This additional staffing reduced the average wait time from 10–30 minutes to less than one minute.

Equifax has continued to make enhancements to the call centers, such as: providing additional training and ongoing updates for agents; adding staff to oversee call center processes; conducting regular and ongoing calls with vendors to discuss agent issues and IT issues; having company leadership visit call centers; conducting agent focus groups; and adding call back functionality to the process.

4. In your written testimony you reference two of your call centers in Florida being taken offline due to Hurricane Irma. Did you alert Experian or TransUnion? Couldn't they have taken some of the load if consumers wanted to activate an initial fraud alerts?

Response: Please see the response to Question 3. Equifax tripled its call center team and was continuing to add agents even as it faced some difficulty due to Hurricane Irma. Equifax did not alert Experian or TransUnion concerning the call centers being affected by Hurricane Irma.

5. How many consumers have signed up for Equifax credit freeze services since September 7, 2017?

Response: As of January 23, 2018, approximately 3.56 million consumers had signed up for Equifax credit freeze services.

6. Will Equifax be refunding fees or charges to potentially impacted customers who enrolled to freeze their credit reports after the breach but prior to September 7, 2017?

Response: Equifax has waived the fee to add, lift, or permanently remove security freezes implemented by consumers on an Equifax credit file from 5pm Eastern on September 7, 2017 through January 31, 2018. Equifax refunded any charges incurred by consumers to place a security freeze on their Equifax credit file between 5:00 pm EST on September 7, 2017, and the announcement of the fee waiver on September 9, 2017.

Written Questions for the Record from the Honorable Jan Schakowsky

1. In your written testimony, you stated that Equifax will offer a new free credit lock product that "has been under development for months" and will be available by January 31, 2018. The free TrustedID Premier package currently offered to consumers in the wake of the breach already includes a credit lock tool. And I understand that outside of the TrustedID Premier package, Equifax had been offering a monthly subscription service for locking and unlocking.

a. We have been told that this free credit lock tool that will be available by January 31, 2018, could require consumers to consent to Equifax sharing or selling the information it collects from the service to third parties. What third parties will Equifax share or sell information collected about consumers from their use of this new credit lock tool?

Response: Equifax does not plan to sell information collected through the Lock & Alert service to third parties. However, Equifax will need to share the information that it collects with third parties necessary to assist with the service. For example, if Equifax uses a third party vendor to assist with verifying an individual's identity, the company will share the information necessary for the vendor to assist with that identification.

b. Equifax is not currently offering any new subscription products. But for the credit lock product that Equifax had been offering as a subscription product, how much did that service cost per month? How many locks and unlocks were permitted per month in that program? What was the total cap on locks and unlocks under the program?

Response: Prior to September 7, 2017, Equifax offered several products with credit lock features. For example, the Equifax Complete Premier product, which included a Credit Report Control feature, cost $19.95/month. There were no limits or caps on locks and unlocks using that product.

c. Why has it taken months to develop the new credit lock tool that will be offered by January 31, 2018, when you already have credit locking tools available?

Response: The new credit lock tool that will be offered on January 31, 2018, is not only web-enabled like current options, but is also accessible through a mobile application, or app. Equifax's new app will empower consumers to better control certain access to their Equifax credit file directly, on their mobile phones—for free, for life.

i. In addition to the cost, please detail with specificity the differences between the new free credit lock tool that Equifax will begin offering in January and the credit lock tool that had been offered as a subscription service. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ

with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.

Response: The new Lock & Alert is a user-friendly service that allows consumers to lock and unlock their Equifax credit files using the mobile app or online. The overall Lock & Alert experience is streamlined to focus on the lock/unlock functionality, and the User Interface is designed to make that experience simple.

ii. You testified at the hearing that the credit report lock that is part of TrustedID Premier is only web-enabled and that the credit lock tool that will be available by January 31, 2018, will be an application. Please explain that comment in more detail. In addition to that difference, please detail with specificity all other differences between the credit report lock that is part of TrustedID Premier and the credit lock tool that will be available by January 31, 2018.

Response: The TrustedID Premier product is web-enabled, meaning that the consumer must use a web browser to log on and access the features. The new Lock & Alert service will not only be web-enabled, but also will be available via the download of a mobile app from the Apple and Google Play stores. The new Lock & Alert service provides consumers with the ability to lock and unlock their credit reports directly from their mobile phones. It will send an alert (by email and/or SMS) to consumers each time their lock status is changed. Lock & Alert is purpose-built to educate consumers about credit locks and to make the process of locking and unlocking credit files as user-friendly as possible. Both the TrustedID Premier product and the Lock & Alert also permit consumers to lock and unlock their credit files by phoning the call center.

1d. How does a credit lock differ from a credit freeze?

i. Please detail with specificity the differences between the credit lock tool that Equifax had been offering as a subscription service and a credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.

ii. Please detail with specificity the differences between the credit lock tool that is part of TrustedID Premier and a credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.

iii. Please detail with specificity the differences between the new free credit lock tool that Equifax will begin offering in January and a

credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.

Response: At the most basic level, the lock and freeze do the same thing: they prevent certain access to your Equifax credit report by creditors and lenders, and help prevent the opening of unauthorized new accounts. Unless a consumer gives permission or takes an action, such as removing or lifting the freeze or unlocking, a lender or other creditor cannot access the consumer's Equifax credit report with a security freeze or a credit file lock in place.

Security freezes (also known as credit freezes) use a PIN based system for identity authentication. Credit file locks are mobile-enabled, and use usernames and passwords for authentication. Detailed directions for freezing or locking an Equifax credit file are set forth on the company's website. The directions are paraphrased below:

Lock – One way to lock your Equifax credit file is by enrolling in TrustedID Premier. This identity theft protection and credit file monitoring service is free for one year to all consumers who enroll by January 31, 2018. Once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, login and simply click the lock button. There are some exceptions where a lock may be delayed or may not be possible.

To unlock an Equifax credit file, once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, log in and simply click the unlock button.

Beginning on January 31, 2018, consumers may also enroll in the new Lock & Alert service to lock their Equifax Credit File. The Lock & Alert service will give consumers the ability to lock and unlock their Equifax credit reports for free, for life.

Freeze – An Equifax security freeze can be placed by mail, phone, or online. Equifax has waived the fee to add, lift, or permanently remove a security freeze through January 31, 2018. Any freeze activities after January 31, 2018 may be subject to the fees provided by your state of residence. The easiest and fastest way to freeze your Equifax credit file is by using Equifax's online process found at the following link: www.freeze.equifax.com. If you choose, you may also request a security freeze by calling Equifax's automated line at 1-800-685-1111. NY residents please call 1-800-349-9960. You may also submit your request in writing to:

Equifax Security Freeze
P.O. Box 105788

Atlanta, Georgia 30348

When you freeze your Equifax credit file, you will receive a 10-digit randomly generated PIN from Equifax that you will need to save and have available should you choose to temporarily lift or permanently remove the freeze in the future.

iv. **A. For Equifax's credit lock tool that will be available by January 31, 2018, please specify the provisions of each state regulation that the credit lock tool will not have to comply with but that credit freezes do have to comply with.**

iv. **B. Please explain in detail why a username and password is a better experience than a PIN-based system for users. Please explain how usernames and passwords are more secure than PINs.**

Response: Equifax has a freeze service that varies by state and complies with each state's statutory requirements, and will continue to offer that security freeze service pursuant to state law. While similar in that it restricts certain access to a consumer's Equifax credit file, Lock & Alert is a common experience for all consumers and free service that uses online and mobile app technology. It does not require a PIN.

Generally speaking, with company-generated PINs (especially where longer than 8 characters) it is difficult for consumers to commit the PIN to memory, and so consumers feel the need to record the PIN in some manner—often written down, stored unencrypted on devices, even on a slip of paper stored in a wallet or purse. With the Lock and Alert service, Equifax requires consumer-generated complex passwords with these requirements:

- Must be between 8 and 20 characters
- Must contain both upper and lower case letters
- Must contain at least 1 number
- Must contain at least 1 special character
- Cannot contain more than 2 repeating characters
- Cannot contain the user name
- Cannot contain 9 or more consecutive numbers
- Cannot contain spaces
- Cannot use "remember me"

Password strength is a measure of effectiveness of a password against guessing or brute-force attacks. The complexity of the password construct Equifax created for this service adds to its strength—it takes into consideration length, complexity, and unpredictability.

1e. Yes or no: will the credit lock tool that will be available by January 31, 2018, require consumers to agree to a mandatory arbitration clause to use the tool? Please provide a copy of the anticipated terms of service for this tool or detail with specificity the terms of service that Equifax expects will be associated with this tool.

Response: No. Equifax will not include an arbitration clause in connection with the forthcoming credit lock service that will be available on January 31, 2018. The terms of service for the forthcoming credit lock service have not been finalized.

1. In your written testimony, you stated that Equifax will offer a new free credit lock product that "has been under development for months" and will be available by January 31, 2018. The free TrustedID Premier package currently offered to consumers in the wake of the breach already includes a credit lock tool. And I understand that outside of the TrustedID Premier package, Equifax had been offering a monthly subscription service for locking and unlocking.

f. Consumer Reports has said, "In most cases a credit freeze offers better protections against fraud, making it the best option." Do you agree with Consumer Reports? What rights and recourse does a consumer have if the lock system fails? What rights and recourse does a consumer have if a credit freeze fails? Please specify by state as necessary.

Response: A credit report lock and a security freeze both generally prevent unauthorized access to a consumer's credit report to open new credit accounts. Credit freezes (also known as security freezes) can be placed or removed online, by phone, or by mail, and use a PIN-based system for identity authentication. Credit file locks are available online or via mobile application, and use usernames and passwords for authentication. Each consumer should evaluate the options and determine which option is right for them. The rights and recourse applicable in the event that a credit freeze fails would depend on the facts of a particular situation, but generally, credit freezes are governed by state statute or regulation, while credit file locks are contractual in nature. For additional information, note that the FTC has published a FAQ and comparison chart regarding locks, freezes, and alerts. It is available at https://www.consumer.ftc.gov/blog/2017/12/fraud-alert-freeze-or-lock-after-equifax-faqs.

1g. How specifically does a credit lock help prevent the consequences of identity theft that are not related to opening new lines of credit, such as fraudulent tax refunds, fraudulent insurance claims, and the many other types of fraud that may occur?

Response: The new Lock & Alert Service restricts access to consumers' credit reports. Credit locks and freezes do not generally serve the purpose of combating other types of identity theft unrelated to credit and credit report information, such as fraudulent tax refunds, fraudulent insurance claims, and some other types of fraud.

1h. Consumers can still choose to freeze their credit instead of using a credit lock tool. For those consumers, other than those living in states with fee limitations, how much does it cost to freeze their credit? How much does it cost to unfreeze their credit?

Response: Costs associated with security freezes are subject to state regulation. Fees for freezing or unfreezing a credit file vary from state to state and can also vary within a particular state depending on factors such as the age, disability, or active duty military status of a consumer and whether the consumer has been a victim of identity theft. Equifax has waived fees associated with placing, temporarily lifting, or permanently removing credit freezes on a consumer's Equifax credit file through June 30, 2018.

2. Equifax is offering consumers one free year of a package of services called Trusted ID Premier. It includes credit monitoring at the big three CRAs, copies of your Equifax credit report, identity theft insurance, Internet scanning for your Social Security number, and the ability to lock and unlock your Equifax credit report.

a. Yes or no: do you expect all attempts at identity theft to occur within one year of this breach?

b. Why isn't Equifax offering Trusted ID Premier for longer than a year?

Response: It is impossible to know whether attempts at identity theft will occur. Equifax believes that the best way for consumers to protect themselves and prevent any harm from fraudulent activity is to enroll in TrustedID Premier, enrollment in which has been offered for free to all U.S. consumers since September 7, 2017, and will be available through January 31, 2018. Consumers can further utilize the free lock service beginning on January 31, 2018, which will give consumers the ability to lock and unlock their Equifax credit report not just for one year, but rather for free, for life.

c. Within the year that consumers may have the TrustedID Premier service, how specifically does that package of services help prevent the consequences of identity theft that are not related to opening new lines of credit, such as fraudulent tax refunds, fraudulent insurance claims, and the many other types of fraud that may occur?

Response: The TrustedID Premier service does not combat the types of identity theft unrelated to credit and credit report information, such as fraudulent tax refunds, fraudulent insurance claims, and some other types of fraud.

d. How will Equifax compensate victims for each of the potential consequences of identity theft? Has Equifax set aside funds to compensate victims for things like insurance and legal costs? If so, how much has been allocated? If not, do you plan to do so?

Response: Equifax believes that the best way for consumers to protect themselves and prevent any harm from occurring is to enroll in TrustedID Premier and utilize the free lock service beginning on January 31, 2018.

Equifax is committed to working with the entire industry, including Experian and TransUnion, and with Congress, to develop solutions to cybersecurity and data protection challenges.

3. Please provide a copy of or describe with specificity the security incident response plan or protocol that Equifax had in place at the time the breach was discovered at the end of July 2017. Was that plan or protocol followed exactly? If not, please specify each step of the protocol that was not complied with and what actions or inactions occurred instead.

Response: Equifax's Cyber Threat Center ("CTC") is responsible for monitoring, consolidating, and correlating data from all Equifax security monitoring systems, 24 hours a day, 7 days a week. Equifax's CTC responds to, and assesses the seriousness of, numerous cyber security threats every day.

When a cybersecurity incident is identified, the Company's written protocols set forth best practices for responding to the cyber security incident. Equifax's written plans and policies to address cybersecurity incidents include the Security Incident Handling Procedure Guide (the "Incident Guide") and the Security Incident Response Team Plan ("SIRT Plan"). Both of these documents were produced to the Subcommittee on January 26, 2018 (Bates-numbered EFXCONG-EC000000552 to EFXCONG-EC000000605). The documents are also described in more detail above, in response to Latta Question 4d.

Equifax also had a Security Incident Response Standard in place in July 2017, which requires, among other things, that employees report as soon as practical to their manager or to the CTC all known or suspected security vulnerabilities, weaknesses, violations, and unauthorized disclosure of information classified as Confidential or higher. If reported to a manager, the manager must escalate any reported issue to a member of the Company's Security team as quickly as possible. Known or suspected security breaches must be reported in the same manner regardless of location of the breach, including within the Company or within a third party holding the Company's information. If the security event or incident involves a user's immediate manager, the user may report the incident to his or her manager's next level of supervision, another manager, the CTC, or to the CSO.

The Security Incident Response Standard defines a "Security Incident" as the violation of an explicit security requirement resulting in the interruption of or interference with any part of the business, including processes, services, and systems. The Security Incident Response Standard provides several examples of types of Security Incidents, including system failures, phishing emails, sending information inappropriately through email, denial of service attacks, unauthorized or improper access of information, physical damage to company assets, theft, loss, property damage, bomb threats, and natural and man-made disasters.

A copy of the Security Incident Response Standard has been provided with this submission and Bates-numbered EFXCONG-EC000002449 to EFXCONG-

EC000002454 on the enclosed CD, which has been encrypted. The password to gain access to the documents will be sent by separate correspondence.

The suspicious network activity that was identified on July 29, 2017 was timely reported to members of the Security team in accordance with the Security Incident Response Standard. Following identification of the suspicious activity, the Company implemented countermeasures to contain the incident, including blocking IP addresses and taking the affected system offline, while it investigated the incident. Over the next several weeks, Equifax's cybersecurity firm retained by its outside law firm analyzed forensic data seeking to identify and understand these early indications of unauthorized activity on the network. The cybersecurity firm provided Equifax with an executive summary, a supplemental report, and a final supplement summarizing its investigative activities and findings, all of which have been provided to the Subcommittee previously.

4. Please provide a copy of or describe with specificity the breach response protocol and/or Crisis management protocol that Equifax had in place at the time the breach was discovered at the end of July 2017. Was that protocol followed exactly? If not, please specify each step of the protocol that was not complied with and what actions or inactions occurred instead.

Response: Please see response to Schakowsky question 3.

5. Under the security incident response plan or protocol, the breach response protocol and/or crisis management protocol, or any other protocol in place at Equifax at the time the breach was discovered at the end of July 2017, at what point was the Chief Financial Officer to be notified of a breach? Under such protocols, were outside counsel and outside security firms to be hired before the CFO was notified? Is that standard industry practice?

Response: The security team reported to Equifax's Chief Security Officer ("CSO") and operated using defined plans and procedures for responding to security incidents, which were revised on a regular basis. The CSO then determined whether and when any particular cybersecurity incident should be reported to others including the Chief Legal Officer (to whom the CSO reported at the time), the CEO's office, other senior executives, and the board of directors. Equifax's security incident response protocol does not address at what point the Chief Financial Officer is to be notified of a breach, nor does the protocol assign a particular role to the CFO for responding to cybersecurity incidents.

6. In the wake of this most recent breach, customers were directed to an Equifax customer support website, www.equifaxsecurity2017.com. Security researchers have been critical of the website. Some browser security tools blocked the site because it looked fraudulent. It had improper TLS security certificates-an online technology used to transport critical data like Social Security Numbers, which the site was collecting. Further, the domain name was not even registered to Equifax. Consumers have reported that the website keeps crashing or loads slowly.

a. You testified at the hearing that Equifax is not providing most breach victims with any notice of the breach other than this website. This site is the only way for consumers to find out if their data was stolen. It is also the only place they can sign up for the free identity theft protection. Why is it still unreliable more than a month after the breach was made public?

b. Why was it not a higher priority at Equifax to ensure your consumer response website worked well and was secure? If Equifax was too overwhelmed in to do so internally, why didn't you hire an outside firm to build a secure site for consumers?

Response: Equifax did prioritize consumer support and has continuously worked to enhance and improve consumers' experience with the incident website, www.equifaxsecurity2017.com. The Company created more intuitive navigation on the microsite and reduced the number of phone numbers listed. Following the initial launch of the "Am I impacted?" search tool on September 7, 2017, the Company resolved some technical issues with the search functionality. Following the completion of a forensic investigation on October 2, 2017, the Company is now able to provide a more definite impact response to U.S. consumers that take advantage of the "Am I impacted?" search tool, which can be accessed by going to the home page of the site.

In addition, following completion of the forensic investigation on October 2, 2017, the Company has:

- Mailed written notices to the approximately 2.5 million additional U.S. consumers that were potentially impacted; and
- Updated the "Am I impacted?" search tool, on the website to include the entire impacted population of approximately 145.5 million U.S. consumers.

Equifax also has made the website more user-friendly by translating it into Spanish and adding links to helpful information and FAQs.

Finally, the domain name of the website is registered to TrustedID. In 2013, Equifax acquired TrustedID, a company that offers credit file monitoring and identity theft protection products. Equifax's website states: "We want to reassure all consumers going through the enrollment, scheduling and activation process that the TrustedID name in the URL and in the email address are valid."

6c. When a consumer attempts to sign up for TrustedID Premier, and chooses to answer the many questions required, the consumer is told after submitting the online forms that he or she will receive an email with a link to finalize and activate the product and that there may be a delay before receiving that email. There is no immediate confirmation email that the consumer's interaction with Equifax was even successful so the consumer does not know when or if she will hear back. When should a consumer assume the first interaction was not successful and try again? Why did you decide against having a confirmation email sent to the consumer?

Response: Equifax has continued to make improvements to the enrollment process and consumers can now expect to receive their activation email within minutes of completing the registration. If a consumer does not receive their activation email, they should search in their spam/junk folders as some consumers have reported their email provider filtering the activation emails. If the activation email is not received with 24 hours, consumers should contact the call center so agents can assist them in completing their enrollment.

6d. Why did Equifax set up a new website that is completely separate from the Equifax.com for the consumer response to the breach? Did you consider having the consumer response information on your main homepage at Equifax.com? If the main site could not handle the consumer volume, why not just improve your original site if it was insufficient?

Response: Equifax's decision to set up a new website to address the security incident was to ensure compliance with state data breach statutes and provide clear and conspicuous notification and information on the incident to all consumers.

7. Equifax's Twitter account had directed consumers to a fake version of the consumer response website multiple times.

a. Who is responsible for Equifax's Twitter page? What information or training was provided to that person or persons with regard to the breach and Equifax's response to the breach?

b. What steps has Equifax taken to ensure such misinformation will not happen again?

Response: Equifax's communications team is responsible for the Company's social media communications, including Twitter. A vendor agent, who was hired by Equifax to assist with the company's response to consumers, mistyped the name of the website Equifax had set up. Instead of using a macro or template to respond to social posts, the agent was manually typing responses. For posts such as these, Equifax relies on pre-approved content. The agent's actions of providing manually drafted answers via Twitter were against Equifax policy. The agent was terminated when this issue was identified, and the incorrect information was quickly taken down.

8. Equifax has now reported that the personal information of approximately 145.5 million Americans was affected by this breach. You explained in your testimony that access to that personal information occurred through Equifax's on line dispute portal. But most of people whose information was stolen had never used the on line dispute portal at any time in the existence of the portal nor had most of them ever filed a dispute with Equifax through another means. Please explain in detail how the hackers were able to access and acquire the information of 145.5 million Americans by gaining access through the consumer-facing online dispute portal.

a. Where was the accessed information stored? Was all the information available to the dispute portal or were the hackers able to move through Equifax's systems?

b. What specific datasets or systems were accessed by the hackers using the dispute portal?

Response: As part of the incident, the attackers were able to access records across numerous tables with inconsistent schemas. The forensic investigation was able to standardize columns containing various types of sensitive information (listed below). These represent the data fields across attacker-accessed tables that were identified as potentially containing PII. The list of data elements is not exhaustive of all possible data elements in a given table, but instead represents the common PII data elements in the attacker queries.

With the foregoing in mind, the list of data elements is as follows:

- SSN
- First Name
- Last Name
- Middle Name
- Suffix
- Gender
- Address
- Address2
- City
- State
- ZIP
- Phone
- Phone2
- DL #
- DL License State
- DL Issued Date
- D.O.B.
- Canada SIN
- CC Number

- Exp Date
- CV2
- TaxID
- Email Address
- Full Name

Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental report, and a final supplement. For your reference, Equifax has provided copies of the executive summary and supplemental report to the Committee.

8c. According to equifaxsecurity2017.com, "criminals also accessed credit card numbers for approximately 209,000 U.S. and Canadian consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers." Are those additional consumers included in the current 145.5 million number?

Response: For the most part, the additional consumers were included in the 145.5 million number; however, Equifax encouraged consumers to also check the "Am I impacted?" search tool on the home page of the company's website.

9. Limiting access to credit even for a short period of time can have real financial consequences, especially for low-income populations. How quickly will a credit file be able to be locked and unlocked with the feature expected in January and how will you ensure that speed? For example, Equifax was not able to handle the calls coming in from this breach. How can we be sure it will be able to lock and unlock quickly for the entire population of consumers?

Response: Please see response to Question 1c. As explained by Equifax interim CEO Paulino do Barros, Jr. in his September 2017 op-ed in the *Wall Street Journal*, the new service being developed by Equifax and others will allow consumers to easily lock and unlock access to their Equifax credit files. Consumers will be able to do this at will, on their own mobile devices. The new credit lock tool will empower consumers to control access to their Equifax credit file directly—for free, for life. As Mr. Barros explained, the new service is a much improved, more user-friendly service than former products that have been made available to consumers. The new credit lock tool will enable consumers to use their smartphone or computer to lock and unlock their Equifax credit file directly and quickly.

10. Please confirm that under the credit lock tool that will be available by January 31, 2018, consumers will be able to unlock or lock only their Equifax credit file for free for an unlimited number of times per month for their lifetimes. Please confirm that consumers will be able to sign up for this free service at any time in the future.

Response: Beginning in late January 2018, consumers will have the ability to lock and unlock their Equifax credit report for free, for life. Consumers will be able to sign up for this free service at any time in the future.

11. Equifax is only one consumer reporting agency (CRA) out of dozens and one of four major CRAs.

a. Do you agree that locking or freezing at only one agency will leave consumers at risk?

Response: Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges. Equifax is currently offering consumers TrustedID Premier, a free package of services that it believes will substantially mitigate any risk of harm to consumers. Beginning on January 31, 2018, consumers will have the ability to lock and unlock their Equifax credit report for free, for life.

b. Yes or no: will Equifax pay for free credit freezes at the other CRAs or reimburse victims for the money they have to spend to freeze or lock their credit at other CRAs? Yes or no: will Equifax pay for victims to temporarily lift credit freezes as needed?

Response: No. Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges.

The details concerning what Equifax is providing for consumers are set forth on the www.equifaxsecurity2017.com website. TrustedID Premier provides consumers with copies of their Equifax credit report; the ability to lock their Equifax credit report; 3-Bureau credit monitoring of their Equifax, Experian, and TransUnion credit reports; Internet scanning for their Social Security number; and identity theft insurance. Equifax has allowed, and until January 31, 2018 will continue to allow, consumers to enroll in TrustedID Premier for free, and the service lasts for a full year. Beginning on January 31, 2018, consumers will have the ability to lock and unlock their Equifax credit reports for free, for life.

c. Do you support a quick one-stop freeze and unfreeze concept so that consumers can freeze their credit at all agencies at once?

Response: Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges. Equifax is offering consumers TrustedID Premier, a free package of services that it believes will substantially mitigate any risk of harm to consumers. Beginning on January 31, 2018, consumers will have the ability to lock and unlock their Equifax credit report for free, for life.

12. Equifax was hit this time, but all consumer reporting agencies are targeted by cybercriminals because of the vast amount of valuable personal information they possess. Since this is an industry-wide threat, do Equifax and other CRAs share threat information with each other or work together to prevent cyber threats?

Response: Equifax is working with industry partners, including the other two national credit bureaus, to share best practices in the area of cyber security. Since September 7, 2017, Equifax has increased its engagement with other industry participants to convene discussions with an intention to benefit consumers and the financial marketplace.

13. Credit report accuracy has historically been a big problem for CRAs, and consumers have often had trouble getting CRAs to correct mistakes in their reports.

a. What is Equifax doing to ensure it can respond promptly and accurately if more credit reports need to be corrected as a result of this breach?

b. If victims of this breach do have fraudulent items on their credit report, what is Equifax doing so that the victims can feel secure submitting documents to your dispute resolution website if they have to?

Response: Equifax and consumers have an aligned interest in ensuring credit report accuracy; it is in Equifax's business interest to maintain a high level of accuracy in the reports that it provides to lenders and other authorized customers. As such, Equifax is prepared to respond to consumer disputes and has posted a short video to assist consumers at www.equifax.com/personal/disputes. Consumers may also dispute information on their credit files by calling 866-349-5191.

14. Equifax notified the Federal Bureau of Investigation on August 2, 2017, that a cyberattack on a portal containing consumer information had occurred. The Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) were not notified until September 7, 2017, the same day Equifax made the public announcement of the breach. You testified already that you were informed by August 15, 2017, that personally identifiable information was likely stolen. Why did Equifax not notify the FTC or CFPB earlier?

Response: Equifax notified the Federal Trade Commission and the Consumer Financial Protection Bureau via phone calls on September 7, 2017, at approximately the same time Equifax published its official press release announcing the cybersecurity incident. In addition, at the time of the press release, Equifax provided written notifications to 52 state attorneys general on September 7, 2017. Upon the completion of the forensic investigation, Equifax also provided supplemental notifications to those 52 state attorneys general on October 12, 2017. Equifax continues to cooperate with these regulators and law enforcement agencies, among others, in connection with the cybersecurity incident. The company is actively engaging with and being responsive to regulators, federal agencies, and legislators and expect to continue to do so in the future.

15. You wrote in your testimony that you "are ultimately responsible for what happened on [your] watch" at Equifax. Yet the term being used to describe your exit last week after 12 years with the company is "retired"—not resigned or fired. Equifax's board has reportedly retained the right to retroactively classify your departure as "being fired for cause."

a. What conditions would lead the board to redefine your exit as "being fired for cause" rather than "retiring"?

Response: Mr. Smith retired from Equifax without bonus and without severance. The Board and Mr. Smith agreed to defer the characterization of his departure until the Board completes its review of the cybersecurity incident.

Various agreements applicable to Mr. Smith's compensation—including his Employment Agreement and agreements related to Long Term Incentive Awards he received over time—are available publicly as part of the Company's filings with the SEC. The Company also has policies allowing for "clawback" of previously awarded compensation in certain circumstances, generally related to a restatement of financial results. The Board of Directors is engaged in a process to examine each of these provisions.

b. Is there a deadline after which the classification of your exit from Equifax cannot be altered?

Response: The Board and Mr. Smith agreed to defer the characterization of his departure until the Board completes its review of the cybersecurity incident.

c. Was your testimony at the hearing on October 3, 2017, a condition for your ability to "retire" and retain your compensation package?

Response: Mr. Smith unconditionally and voluntarily agreed to appear at the Committee's October 3, 2017 hearing without compensation.

d. Roughly how much of your compensation would you retain even if you were retroactively fired for cause?

Response: As noted in response to Question 15(a), there are various agreements applicable to Mr. Smith's compensation, and the Company has a clawback policy that is outlined in the Company's proxy. The Board is engaged in a process to examine each of those provisions. However, Equifax understands that Mr. Smith's vested pension and supplemental retirement plans are not subject to change. Those plans and Mr. Smith's vested interest in them are also described and set out in the Company's proxy.

16. You wrote in your testimony that the board was involved in the development of Equifax's consumer response after you notified it of the breach in late August.

a. Did the board approve the original and insufficient "consumer notification and remediation program" that Equifax rolled out on September 7?

b. Did the board approve the multiple-week delay in notifying customers of the breach?

Response: Equifax's Lead Director was notified of the cybersecurity incident in a phone call on August 22, 2017, and the full Board was informed in subsequent special telephonic board meetings on August 24 and 25. Between those initial calls and the Company's September 7 public disclosure, the Board was kept informed of the Company's plans for notifying consumers and developing remediation protections for consumers.

17. Equifax needs to reexamine and substantially improve the way it treats consumers. I am concerned that the company has chosen to replace you as Chairman with a board member, Mark Feidler, who was part of Equifax's botched response-and even served on the board's Technology and Governance committees during the breach.

a. What was Mr. Feidler's role in developing and implementing Equifax's consumer response to this breach in August and September?

Response: Mr. Feidler was Presiding Director of the Board of Equifax in August 2017 and became non-Executive Chair in September 2017, a position he holds today. In September 2017, the Board of Directors formed a Special Committee to review the trading in Company securities by certain executives and to conduct an independent review of the cybersecurity incident and the Company's response. A copy of a report by the Special Committee addressing trading is enclosed with this submission.

b. You are an unpaid advisor to Equifax right now, and your association with the company ends in less than three months. But the effects of this breach will be felt by consumers long after that. Will the company commit to having its interim CEO, and the new permanent CEO when one is hired, come back to this committee to provide further updates if necessary?

Response: Equifax is committed to rebuilding the trust of consumers, customers, partners, investors, regulators, and Congress and will continue to respond to committee requests.

18. A patch for the vulnerability that lead to the breach was issued on March 8, 2017, and Equifax confirmed that it was aware of the patch at that time and worked to identify and patch vulnerable systems. You testified that the Equifax security department required this vulnerability to be patched within 48 hours, consistent with the Equifax Patch Management Policy. But you testified that the vulnerability was not identified or patched.

a. Please provide in detail the organizational structure of Equifax at the time of breach, including the entire reporting structure below the Chief Security Officer, the entire reporting structure below the Chief Information Officer, the reporting structure from the Chief Security Officer to the Chief Executive Officer, and the reporting structure from the Chief Information Officer to the Chief Executive Officer.

Response: Equifax is providing with this response copies of organizational charts (EFXCONG-EX00000606 to EFXCONG-EX00001340) that reflect the reporting structures below the Chief Security Officer and the Chief Information Officer at the time of the cybersecurity incident. At that time, the Chief Security Officer reported to the Chief Legal Officer, who in turn reported to the Chief Executive Officer. The Chief Information Officer reported directly to the Chief Executive Officer.

b. It is my understanding that the Chief Security Officer reported to the Chief Legal Officer/General Counsel. Is that common practice in the credit reporting industry? Is that common practice in the data broker industry?

Response: Equifax is not in a position to opine on what is or is not common practice in the credit reporting or data broker industries. Many factors are taken into account when developing an internal corporate structure. Currently, with the assistance of third-party experts, Equifax is performing a thorough review of its security program, including the corporate structure of the Security department. At this point, the interim Chief Security Officer reports to the interim Chief Executive Officer.

c. Who within the company knew or should have known on which applications Apache Struts was running? Who within the company maintained the master list of all applications and what software was running on each application?

Response: At the time the U.S. CERT alert regarding the Struts 2 vulnerability was received in March 2017, one or more of the individuals responsible for developing an Equifax portal knew or would have known of its use of Apache Struts and application developers responsible for developing an application would have been responsible for knowing what software runs as part of that application.

18d. Please describe with specificity Equifax's patch management policy that was in effect in March 2017. What changes have been made to that policy since the breach was discovered in July 2017?

e. Please describe with specificity Equifax's process as of March 8, 2017, for applying patches and verifying that a patch had been applied correctly. Please include what person, position, or office is responsible for each step in that process. Specify the role of the application development team (including the reporting structure), the role of the infrastructure team (including the reporting structure), and the role of the security team (including the reporting structure).

f. In March 2017, where in the internal chain of command did primary responsibility for correctly installing updates fall? Was there an escalation process if a patch was not applied promptly and correctly?

g. The current Chief Security Officer told committee staff that when notified of a vulnerability that required a patch, the application development team would initiate a change ticket for the patch and the infrastructure team would implement the patch. Then a security scan would be run to ensure the patch was applied.

i. Yes or no: is this an accurate statement of the patching process? If no, please explain.

ii. Who received notifications when a change ticket was not completed?

iii. Did the application development team, the infrastructure team, the information technology team, or any team/department other than the security team who reported to the Chief Security Officer have a method of determining that patches were applied? If so, please explain in detail with regard to each team/ department/ office that had such methods.

Response: The Company's Patch Management Policy in place in March 2017 categorized patches into four severity groups: critical, high risk, medium risk, and low risk. The policy required that critical patches be applied within 48 hours, high risk patches be applied within 30 days, medium risk be applied within 90 days, and low risk patches be applied within one year of notification. In situations where a patch could not be applied within the given time period, the policy required that Security be consulted and an alternate time period be mutually agreed upon.

Under the policy, following the installation of a critical patch, Security must re-scan within 48 hours to validate that the patch was successful in remediating the vulnerability.

The Company's Patch Management Policy was last modified in May 2017. For your reference, Equifax is providing a copy (EFXCONG-EC000001341 to EFXCONG-EC000001351) to the Subcommittee with this submission.

At the time the breach was discovered, David Webb was Equifax's Chief Information Officer and Susan Mauldin was Equifax's Chief Security Officer. The individual who oversaw the team responsible for patching the relevant Apache Struts vulnerability on software supporting Equifax's online disputes portal reported to Mr. Webb.

18. A patch for the vulnerability that lead to the breach was issued on March 8, 2017, and Equifax confirmed that it was aware of the patch at that time and worked to identify and patch vulnerable systems. You testified that the Equifax security department required this vulnerability to be patched within 48 hours, consistent with the Equifax Patch Management Policy. But you testified that the vulnerability was not identified or patched.

h. The former Chief Security Officer told committee staff that security scans searched for vulnerabilities, not for properly applied patches. She said that an initial scan was run before the patch for the Apache Struts vulnerability was applied and no vulnerabilities were found. The IT team then applied the patches and that team had ways to determine if the patches were applied. Security did not rescan after the patches were applied because no vulnerabilities were found in the initial scan and, therefore, no vulnerabilities would be found after the patches were applied. Yes or no: is this account accurate? If no, please explain.

Response: No, that account is incomplete. Following Equifax's receipt of the relevant scanner signature from its scanner vendor on or about March 15, 2017, Equifax scanned its external facing Equifax IP addresses, including the online dispute portal, for the Apache Struts vulnerability announced on March 8, 2017 (CVE-2017-5638). No affected systems were identified in response to the March 15, 2017 scan. As a result, Equifax Security did not become aware that any systems required patching until after suspicious network activity was detected on July 29, 2017. Specifically, following identification of the suspicious network activity, Equifax Security identified that the intrusion into the impacted system was a result of the exploitation of the Apache Struts vulnerability. Once this was understood, Equifax patched the vulnerability, and together with Mandiant, ensured through additional targeted scanning that the patch was properly applied.

i. Yes or no: was the scan for vulnerabilities the only method of ensuring that patches were applied?

Response: No.

19. Mandiant conducted a forensic investigation of what happened in this incident and produced a report, which was finalized on October 2, 2017. Please provide a copy of the full report.

Response: For your reference, attached to this submission is the Mandiant executive summary, a supplemental report, and a final supplement.

20. Press reports indicate that Mandiant was working for Equifax in March regarding another Equifax breach. That investigation was described internally as "a top-secret project" that you were personally overseeing.

a. Why did you oversee that breach personally and not the breach that was the subject of this hearing?

Response: The Bloomberg story published on September 29, 2017 inaccurately conflates two separate, unrelated cybersecurity events. Mr. Smith was appropriately involved in responding to both incidents.

The events described in the article appear to inaccurately reference fraud incidents experienced by TALX Corporation, a wholly-owned subsidiary of Equifax. TALX Corporation, operating under the trade name Equifax Workforce Solutions, provides human resources, payroll, tax management, and compliance services. These fraud incidents were not related to the recent cybersecurity incident (see, in pertinent part, Mandiant's supplemental report, produced today as an attachment to this response). A brief background summary of these fraud incidents follows:

- TALX experienced fraud incidents during Spring 2016 and Spring 2017.
- During the Spring of 2016, fraudsters used personal information obtained from non-Equifax sources to access employee accounts that used personally identifiable information for the user ID and personal information for the related default PIN. In response to the 2016 unauthorized access, TALX added an additional layer of authentication for the 2017 tax season.
- During the Spring of 2017, TALX received reports of unauthorized access to individuals' W-2s contained within TALX's online platform. This incident did not involve any hacking of Equifax systems, and there was no mass exfiltration of data.
- Mandiant was hired to assist with the TALX fraud investigation. The situation was also reported to law enforcement. Mandiant investigated both events and found no evidence that the fraud incidents involving TALX were related to the cybersecurity incident announced on September 7, 2017.

b. What changes in security practices, procedures, and protocols were made following that March breach as well as the other three most recent Equifax breaches?

Response: Across the enterprise, Equifax has enhanced controls for restricting and governing access to sensitive data within the environment, in addition to employing measures to increase security and further enhance its ability to detect and respond to malicious activity.

Examples of these initiatives include:

- Enhancing vulnerability scanning and patch management processes and procedures
- Reducing the scope of sensitive data retained in backend databases
- Increasing restrictions and controls for accessing data housed within critical databases
- Enhancing network segmentation, to restrict access from internet facing systems to backend databases and data stores
- Deploying additional web application firewalls, and tuning signatures to block attacks
- Accelerating the deployment of file integrity monitoring technologies on application and web servers
- Enforcing additional network, application, database, and system-level logging
- Accelerating the deployment of a privileged account management solution
- Enhancing visibility for encrypted traffic by deploying additional inline network traffic decryption capabilities
- Deploying additional endpoint detection and response agent technologies
- Deploying additional email protection and monitoring technologies

Equifax will continue to make significant investments in data security, including ongoing engagement with cybersecurity experts to evaluate its data security infrastructure and procedures. All of these steps will help to better detect, mitigate, and respond to potential threats now and in the future.

21. Press reports also indicate that Equifax's relationship with Mandiant broke down, but Mandiant had warned that unpatched systems indicate major problems.

a. What specific information and advice did you receive from Mandiant at that time?

Response: Please see the response to Question 20a.

21. Press reports also indicate that Equifax's relationship with Mandiant broke down, but Mandiant had warned that unpatched systems indicate major problems.

a. Did you personally get the warning? Who else in the company received that warning?

b. What steps were taken in response to that warning?

c. If you were unhappy with Mandiant in March, why hire it again?

Response: The Bloomberg story published on September 29, 2017 inaccurately conflates two separate, unrelated cybersecurity events. Mr. Smith was engaged appropriately in both incidents.

In March 2017, Mandiant was engaged to assist with a different, unrelated forensic investigation. The event discovered on July 29, 2017, did not affect the databases used by the Equifax business unit that was the subject of the March event. Mandiant investigated both events and found no evidence that these two separate events were related.

The incident investigated in March 2017 is described below:

> During the 2015 and 2016 tax season (i.e., early 2016 and early 2017, respectively), unauthorized actor(s) were able to login to an employee's W-2 account through mytaxform.com. In order to login to the account, the unauthorized actor(s) used previously stolen credentials and other personal information to ultimately obtain access to the employee's W-2. Equifax systems were not compromised in this incident.
>
> Equifax received a number of reports from employer clients of its tax form management service that some of their employees may have experienced tax fraud in the form of someone attempting to file a tax return in the employee's name.
>
> Equifax investigated each of these reports in order to determine whether there had been any access to the employee's accounts on Equifax's electronic W-2 platform. An independent, third-party cybersecurity firm, Mandiant, was hired to assist with the investigation. The situation was also reported to law enforcement.
>
> Equifax is continuing to work with law enforcement and to investigate this issue to the extent possible.

22. Equifax reported that unauthorized access to consumer data started on May 13, 2017. One large financial firm told the *Wall Street Journal* that it saw a spike in fraudulent activity using the same types of data stolen in the breach starting in late May.

a. Do you know if the criminals have used or sold the data that was stolen? Has Equifax performed any analysis to see if fraud alerts or credit report disputes for your own reports have increased since May?

b. Is Equifax aware of a noticeable increase in synthetic identity theft where the fraudster takes data points from multiple established identities in recent months or years?

Response: In response to the cybersecurity incident, Equifax developed a robust package of remedial protections for each and every U.S. consumer – not just those affected by the breach. The relief package includes (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files; (3) the ability to lock the Equifax credit file, (4) and insurance policy to cover out-of-pocket costs associated with identity theft, and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all U.S. consumers. We believe that the best way for consumers to help protect themselves is to enroll in TrustedID Premier and utilize the free lock product, Lock and Alert.

23. I understand Equifax has changed its reporting structure in the wake of the breach. Please provide in detail the current organizational structure of Equifax, including to whom the new Chief Security Officer reports and to whom the Chief Information Officer reports.

Response: Please see the response to Question 18a.

24. Susan Maudlin, the former Chief Security Officer told committee staff that she informed John Kelley, the Chief Legal Officer, to whom she regularly reported, of the breach by July 31, 2017. She also said that at the same time Mr. Kelley was informed that the incident may have compromised personally identifiable information.

a. Do you and Equifax deny that assertion?

Response: On July 30, 2017, Chief Legal Officer John Kelley was informed that unusual activity had been detected on Equifax's network the prior evening. Mandiant and the Equifax security department did not begin to determine the level of unauthorized activity until mid-August. Accordingly, neither Mr. Kelley nor anyone else at the company was aware of the scope of the intrusion before that time.

b. Is it true that Mr. Kelley is still Chief Legal Officer for Equifax?

Response: Mr. Kelley currently serves as the Chief Legal Officer for Equifax.

25. Your testimony noted a "mounting concern" as of September 1, 2017, that Equifax's system had to be prepared for new "copycat" and other attacks after public notification of the breach.

a. Who informed you of that concern? When were you first informed of that concern? When did Equifax begin preparing its systems for those anticipated attacks? Did Equifax wait until September 1?

Response: In late August 2017, Equifax began preparing its network for "copycat" attacks.

On September 1, Mr. Smith convened a Board meeting to discuss the scale of the breach and what Equifax had learned so far, noting that the company was continuing to investigate. Equifax also discussed its efforts to develop a notification and remediation program that would help consumers deal with the potential results of the incident. Experts informed the company that it had to prepare its network for exponentially more attacks after the notification, because a notification would provoke "copycat" attempts and other criminal activity. This is a general concern that is common whenever a company announces a data breach. Equifax Security, Equifax Legal, Mandiant, and Equifax's outside counsel would all have engaged in various discussions on this topic.

b. What preparations were made for those attacks?

Response: Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident and to help Equifax prepare its network for "copycat" attacks and other criminal activity. Mandiant has provided Equifax with an executive summary, a supplemental report, and a final supplement, which have been provided to the Subcommittee as an attachment to this submission.

26. When and why did you decide that September 7 would be the day you announced the breach?

a. What day were employees at your customer service call centers informed about the breach?

Response: As Equifax reported in its press release on September 15, 2017, the company worked diligently with Mandiant to determine what information was accessed and identify the potentially impacted consumers in order to make an appropriate public disclosure of the incident. As soon as the company understood the potentially impacted population, a comprehensive support package was rolled out to consumers on September 7, 2017. Employees at the customer service call centers were hired and informed of the breach over a period of time:

- In late August 2017, Equifax began developing the remediation needed to assist affected consumers, even as the investigation continued. On August 28, a core team was pulled in to start mobilizing call centers and incident remediation activities, and ten agents were sent to call centers to perform training.

- On September 7, 2017, the same day that Equifax provided notification of the incident by issuing a nationwide press release, additional agents were added, raising the number from 770 to 1,350 call center agents.

- On September 11, 2017, the call center lost approximately 700 staff for two days because of Hurricane Irma. Equifax began the process of hiring 150 people to assist with responding to emails and social media requests.

- On October 6, 2107, Equifax hired an additional 2,045 agents to handle authentication and servicing issues. These employees were cross-trained on TrustedID Premier and security freeze issues.

- On October 27, 2017, Equifax hired 41 additional agents to handle Global Customer Care issues.

26. When and why did you decide that September 7 would be the day you announced the breach?

a. What day were employees at your customer service call centers informed about the breach?

Response: As Equifax reported in its press release on September 15, 2017, the Company worked diligently with Mandiant to determine what information was accessed and identify the potentially impacted consumers in order to make an appropriate public disclosure of the incident. As soon as the Company understood the potentially impacted population, a comprehensive support package was rolled out to consumers on September 7, 2017. Employees at the customer service call centers were hired and informed of the breach over a period of time:

- In late August 2017, Equifax began developing the remediation needed to assist affected consumers, even as the investigation continued. On August 28, a core team was pulled in to start mobilizing call centers and incident remediation activities, and ten agents were sent to call centers to perform training.

- On September 7, 2017, the same day that Equifax provided notification of the incident by issuing a nationwide press release, additional agents were added, raising the number from 770 to 1,350 call center agents.

- On September 11, the call center lost approximately 700 staff for two days because of Hurricane Irma. Equifax began the process of hiring 150 people to assist with responding to emails and social media requests.

- On October 6, Equifax hired an additional 2,045 agents to handle authentication and servicing issues. These employees were cross-trained on TrustedID Premier and security freeze issues.

- On October 27, Equifax hired 41 additional agents to handle Global Customer Care issues.

b. How were call center employees trained to help consumers and answer questions about the breach?

Response: Call center agents received extensive, issue-specific training. Experienced agents were sent to the call centers to train new call center agents. Following the announcement of the breach, Equifax continued to provide additional training and ongoing updates for call center agents.

c. Did you hire additional employees for the call centers before September 7? If not, why?

Response: Yes. Prior to the September 7, 2017 announcement of the breach, Equifax hired approximately 770 incremental call center agents. On September 7, 2017, Equifax added these additional call center agents, bringing the total number of incremental call center agents to approximately 1,350. In order to handle the unprecedented call volume following the announcement of the breach, Equifax continued to increase call center staffing. By October 6, 2017, Equifax had added another 2,045 agents to handle authentication and servicing issues, bringing the total number of incremental call center agents to approximately 3,400. Equifax also continuously solicited overtime and double shifts to increase utilization of call center agents.

26d. When did you start building the website? Had you subjected it to any performance tests or security audits before September 7?

Response: Equifax began building the www.equifaxsecurity2017.com website in August 2017 after the forensic investigation had determined that there were large volumes of consumer data that had been compromised by the breach. Equifax conducted security testing prior to the launch of the www.equifaxsecurity2017.com website in order to ensure that the website was secure before the launch and has continued to perform testing and monitoring of the website following the launch.

27. What could Equifax have done differently to provide consumers with better support and more information earlier? What is Equifax doing now to provide consumers with better support and more information going forward?

Response: The scale of this incident was enormous, and Equifax struggled with the initial volume of consumers utilizing its call centers and websites. The company dramatically increased the number of customer service representatives at the call centers, and the website has been improved to handle the large number of visitors.

Equifax did develop a robust package of remedial protections for each and every U.S. consumer—not just those affected by the breach. The relief package includes (1) monitoring of consumer credit files across all three bureaus, (2) copies of Equifax credit reports, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft, and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all U.S. consumers.

The Company has also announced a new service that will be available by January 31, 2018, that will allow consumers to control their own credit data, by allowing them to lock and unlock their credit files at will, repeatedly, for free, for life.

In addition to the services described above, security freezes, and fraud alerts are available to consumers to help protect against credit fraud.

Finally, credit reporting agencies are an essential—yet little-known—part of the financial ecosystem. Equifax now realizes that it has to do a better job of providing consumers with the tools and resources they may need to understand the role it plays in that system. Equifax also wants to empower consumers with more control over personal credit data, and it wants to collaborate across the industry to give them that control.

28: On August 17, 2017, at least two days after you knew about the breach and that personally identifiable information was compromised, you said in a speech, "[f]raud is a huge opportunity for [Equifax]. It is a massive, growing business for us." What did you mean by that comment?

Response: Mr. Smith made those remarks on the morning of August 17 at the University of Georgia Business School, to meet a long-standing commitment to speak to the school. When he gave the speech, he did not know the size or scope of the breach. One of the services Equifax offered at the time to consumers was credit monitoring and credit locks to assist them in having more control over their credit data. Following Equifax's own breach, the company is now offering those and other services for free.

29. According to media reports, Equifax has had a number of other problems protecting consumers' personal information. There have been a number of incidents in which a customer was inadvertently sent or able to view credit information of other customers. One report indicated that a customer was inadvertently sent hundreds of credit reports, which included personal information, of other consumers. What practices does Equifax have in place to detect and respond to such data leaks and inadvertent disclosures of consumers' personal information?

Response: None of the incidents described in the above question were the result of Equifax systems being compromised.

In the first incident, due to a technical error within the Equifax mailing system, certain consumer information was inadvertently sent to incorrect individuals. The issue was discovered and resolved within approximately 24 hours. An architectural review, onboarding process review, capacity assessment, and successful stress and performance testing were completed.

In the second incident, a small number of consumers were able to view other consumers' credit reports when logged into an Equifax customer member portal over a period of several days. Upon discovery, Equifax's customer suspended all credit report features in their member portal until the issue was resolved. Within 48 hours, Equifax deployed a software fix that eliminated the issue for all existing and new consumer enrollments. The customer then re-enabled the credit report feature on its member portal. Equifax and its customer identified the complete list of impacted consumers, including those having seen another consumer's report, and those who had their report viewed by another consumer. Further, there was no indication that consumer information exposed in this incident resulted in harm to consumers.

In each instance, Equifax moved expeditiously to correct any technical hardware, software, and/or coding issues that resulted in the inadvertent disclosure of consumers' personal information.

Written Questions for the Record from the Honorable Ben Ray Lujan

1a. What, if anything, has been done to address the vulnerabilities on the Equifax website exposed in the data breach?

Response: Equifax has implemented several updates to protocols and procedures in response to this incident. Equifax has made changes to the process by which the Security Global Threat and Vulnerability Management ("GTVM") team notifies the IT team of necessary security patches and system vulnerabilities. The Company is now performing external scans using the Rapid 7 scanner from vendor Nexpose. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company also has implemented additional network, application, database, and system-level logging.

Equifax's forensic consultants have recommended and have implemented a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also retired from their positions.

l . Extensive weaknesses in Equifax's data protection system were revealed after the hacking.

b. Are there now regular audits and other forms of security monitoring currently in place? How often?

Response: As it has done in previous years, Equifax continues to engage third parties to assess and audit its security protection, detection, and response capabilities across the enterprise. In addition to the Company's Security Operation Center, which monitors alerts generated by the Company's security appliances, the Company also has employed third-party vendors to provide additional security monitoring on a 24/7 basis. Equifax conducts monitoring and testing of security-related controls on an ongoing basis, including monthly testing of patch management and data loss prevention controls.

1c. How has the company improved its cybersecurity following the breach?

Response: Equifax engaged PwC, on September 22, 2017, to assist with its security program, including strategic remediation and transformation initiatives that will help the Company identify and implement solutions to strengthen its long-term data protection and cybersecurity posture.

Equifax's forensic consultants have recommended and have implemented a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also retired from their positions.

1d. What will Equifax do to ensure that consumers affected by the theft of their personal information from your system are made whole?

Response: Equifax believes that the best way for consumers to protect themselves is to enroll in TrustedID Premier, a package of services being offered for free until January 31, 2018, and utilize the free Lock & Alert service beginning on January 31, 2018. Providing a free service to lock their files is the best way for Equifax to add value and make consumers whole. Equifax is firmly committed to working with the industry and with Congress to identify ways to protect and empower consumers and to develop solutions to this growing problem.

1e. What does Equifax do to secure its websites? What changes is Equifax putting in place after this most recent website incident, to ensure its websites do not contain malicious links or code?

Response: Across the enterprise, Equifax has enhanced controls for restricting and governing access to sensitive data within the environment, in addition to employing measures to increase security and further enhance its ability to detect and respond to malicious activity. Equifax will continue to make significant investments in data security, including ongoing engagement with cybersecurity experts to evaluate its data security infrastructure and procedures. All of these steps will help to better detect, mitigate and respond to potential threats now and in the future.

2a. What specifically are the differences between the one-year credit freeze now offered and the "credit lock" you will be offering?

Response: Security freezes (also known as credit freezes) use a PIN based system for identity authentication. The new credit lock tool that will be offered on January 31, 2018, is accessible through a mobile app and will use usernames and passwords for authentication. Equifax's new app will enable consumers to use their smartphone or computer to lock and unlock their Equifax credit file directly and quickly—for free, for life.

2b. There have been a number of recent complaints from customers opting to use Equifax's credit freeze service that they have been unable to temporarily lift their credit freezes online or by phone because of various customer service failures. For example, consumers have reported that the automated phone system provides no means of entering a PIN and that they are unable to reach a customer service agent. Others report that website failures prevent them from lifting their freeze online. Could you please provide an explanation? What steps is Equifax taking to ensure that the website is working properly and that customers can easily lift a credit freeze by phone?

Response: The scale of this incident was enormous, and Equifax struggled with the initial volume of consumers utilizing its call centers and website. Equifax is continuously working to enhance and improve consumers' experience with the incident website, www.equifaxsecurity2017.com. The Company created more intuitive navigation on the microsite and reduced the number of phone numbers listed. Following the initial launch of the "Am I impacted?" search tool on September 7, 2017, the Company resolved some technical issues with the search functionality. Following the completion of a forensic investigation on October 2, 2017, the Company is now able to provide a more definite impact response to U.S. consumers that take advantage of the "Am I impacted?" search tool, which can be accessed by going to the home page of the site.

In addition, following completion of the forensic investigation on October 2, 2017, the Company has:

- Mailed written notices to the approximately 2.5 million additional U.S. consumers that were potentially impacted; and
- Updated the "Am I impacted?" search tool on the website to include the entire impacted population of approximately 145.5 million U.S. consumers.

2c. As previously stated, customers could be reeling from theft of their data resulting from this data breach for years. Why has the company not made credit freezes, in addition to credit locks, free in perpetuity for those affected?

2d. What is the rationale for offering a free credit freeze for only a limited period of time, when it's clear the stolen data could be used at any time to create fraudulent accounts and otherwise prey on the victims of this breach? Why should consumers in years to come be forced to pay for Equifax's failure to protect their data in the first place?

Response: It is impossible to know whether attempts at identity theft will occur. Equifax believes that the best way for consumers to protect themselves and prevent any harm from occurring is to enroll in TrustedID Premier, the package of services that Equifax believes will substantially mitigate any risk of harm to consumers. The TrustedID Premier service is being offered for free until January 31, 2018. Beginning on January 31, 2018, consumers will have the ability to lock and unlock their Equifax credit report for free, for life, with Equifax's new credit lock service, Lock & Alert. This service will empower consumers to control access to their Equifax credit file using their smartphone or computer to lock and unlock their Equifax credit file directly and quickly. Equifax will announce additional details of the new credit lock service on January 31, 2018.

Equifax's primary focus is protecting consumers and the businesses Equifax serves. Equifax will continue to engage with consumers, regulators, and lawmakers regarding potential additional measures to mitigate any risk of harm to consumers.

2e. During the hearing, you testified that Equifax was not currently working with the other credit reporting agencies to provide protections for consumers impacted by the data breach. Can you provide an explanation as to why your company is not working with Experian and TransUnion to ensure they provide free credit freezes and other reasonable consumer protections? Can you explain why your company is not offering to pay for credit freezes or other reasonable protections on behalf of consumers at Experian and Trans Union?

Response: Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges. Equifax is offering consumers TrustedID Premier, a free package of services that it believes will substantially mitigate any risk of harm to consumers by helping to prevent unauthorized use of their personal information. Beginning on January 31, 2018, consumers will have the ability to lock and unlock their Equifax credit report for free, for life. Equifax will continue to work with the industry to improve the consumer experience with the national credit bureaus.

3a. During the hearing, you testified that from a customer perspective, a credit lock and credit freeze are the same. If a credit lock and freeze are the same, why doesn't Equifax simply offer credit freezes, which come with strong, well-understood legal protections for consumers, for free?

Response: Please see response to Question 2d.

3b. What information about consumers does Equifax collect, share, sell, or otherwise grant access to third parties under a credit lock that it does not under a credit freeze?

Response: The information Equifax collects for a credit lock is similar to that collected for a credit freeze and includes name, address, date of birth, and social security number. For consumer information collected by Equifax in the registration process for a freeze, see https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp.

For consumer information collected by Equifax in the registration process for a credit lock, see https://trustedidpremier.com/eligibility/eligibility.html.

Locking an Equifax credit file will prevent access to a consumer's Equifax credit file by certain third parties. Locking the Equifax credit file will not prevent access to the consumer's credit file maintained by any other credit reporting agency. Entities that may still have access to a consumer's locked Equifax credit file include companies like Equifax Global Consumer Solutions, which provide consumers with access to their credit report or credit score, or monitor the consumer's credit file; federal, state, and local government agencies; companies reviewing a consumer's application for employment; companies that have a current account or relationship with the consumer, and collection agencies acting on behalf of those whom a consumer owes; for fraud prevention and detection purposes; and companies that make pre-approved offers of credit or insurance to the consumer. Consumers can opt out of pre-approved offers at www.optoutprescreen.com. Similarly, under state freeze laws certain third parties, like those mentioned above, may continue to have access to a frozen Equifax credit file.

Equifax is monitoring federal and state legislation that may impact operations of freezes and locks.

Written Questions for the Record from the Honorable John Sarbanes

1. Can minors have their identity stolen?

Response: Children may be targeted by identity thieves, which may include family members or close family friends. Parents and guardians may take the following precautions to protect their children's identities:

- Keep children's documents in a secure location.
- Before sharing a child's social security number, question why it is needed, how it will be used, and how it will be safeguarded.
- Become familiar with the laws that protect your child's information, such as the Family Educational Rights and Privacy Act, which gives parents of school-age kids the right to opt out of sharing directory information with third parties. More information is available from the U.S. Department of Education at https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

The Federal Trade Commission's website includes additional information about protecting the identity of minors and provides steps to take if a parent or guardian believes their child's identity has been stolen. This information is available at https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

2. Does Equifax offer monitoring and security products to protect minors from identity theft?

Response: Generally an individual under the age of 18 does not have a credit file; however, many states have laws allowing a parent or guardian to request a security freeze for a minor. This process requires the creation, and subsequent freeze, of a minor's credit file if one does not exist. Currently, Equifax is not offering credit monitoring or identity theft protection products for sale to consumers.

3. Were any minors impacted by this latest breach? Please explain how you can be sure.

Response: A small percentage (.19%) of the impacted consumers had a date of birth that would indicate the information may be associated with a minor. While the TrustedID Premier service is not available for minors or those without a current Equifax credit file, Equifax created a process for any parent or guardian that contacted Equifax claiming they had an impacted minor to, if desired, place a special minor lock for the impacted minor.

4. Are minors eligible to receive Equifax's free monitoring services? Please explain how this decision was reached and why.

Response: Many states have laws allowing a parent or guardian to request a security freeze for a minor. TrustedID Premier is only available to adult consumers who have an Equifax credit file**.**

Written Questions for the Record from the Honorable Jerry McNerney

1. Please provide in detail the organizational structure both prior to and after July 29, 2017 of Equifax's Security Department and its Information Technology Department.

Response: Prior to the security incident, Equifax's former Chief Security Officer reported to the Chief Legal Officer and the former Chief Information Officer reported to the Chief Executive Officer. As part of the company's review of the cybersecurity incident announced on September 7, 2017, Equifax made personnel changes and released additional information regarding its preliminary findings about the incident. The company announced that the Chief Information Officer and Chief Security Officer are retiring. Mark Rohrwasser has been appointed interim Chief Information Officer. Mr. Rohrwasser joined Equifax in 2016 and has led Equifax's International IT operations since that time. Russ Ayres has been appointed interim Chief Security Officer. Mr. Ayres most recently served as a Vice President in the IT organization at Equifax. The personnel changes were effective immediately.

The interim Chief Security Officer and the interim Chief Information Officer currently report directly to the interim Chief Executive Officer. Please see organizational charts referenced at the documents Bates-numbered EFXCONG-EC000000552 to EFXCONG-EC000000605.

As of June 30, 2017, the end of the quarter prior to Equifax discovering the cybersecurity incident, there were approximately 232 full-time employees in the Security department and approximately 2,497 full-time employees employed in the Information Technology department. As of December 1, 2017, there were approximately 239 full-time employees in the Security department and 2,600 full-time employees employed in the Information Technology office. In addition to full-time employees, the Security department also engages third parties to assist with information security efforts.

2. What function(s) does the Security Department carry out in the vulnerability patching process?

Response: Equifax produced a copy of the Patch Management Policy (EFXCONG-EC000001341 to EFXCONG-EC000001351) to the Subcommittee on January 26, 2018. That policy outlines the roles and responsibilities for the vulnerability patching process.

3. What function(s) does the Information Technology Department carry out in the vulnerability patching process?

Response: Please see response to McNerney Question 2.

4. According to your oral testimony before the House Energy and Commerce Committee on October 3, 2017, Equifax has 225 cybersecurity professionals. Please list the criteria that must be met in order for an individual to qualify as a "cybersecurity professional" at Equifax. What cybersecurity training are these individuals provided and does Equifax maintain and encourage ongoing cybersecurity training of its employees?

Response: The number of cybersecurity professionals at Equifax was established as the number of employees who are formally part of the Equifax Security team. All Equifax employees have mandatory cybersecurity training at least annually.

5. Do all of the 225 cybersecurity professionals work in Equifax's Security Department or do some of them work in other departments? If in other departments, please specify which departments.

Response: The more than 225 professionals focused on security referenced by Mr. Smith are members of Equifax's Security department; however, other employees are also regularly engaged in information security, including members of the Equifax Technology, Data and Analytics, and Compliance teams. Equifax also uses third parties to assist with information security efforts.

6. Who at Equifax received the U.S. Department of Homeland Security, Computer Emergency Readiness Team's (US-CERT) notification concerning the need to patch the Apache Struts vulnerability?

Response: Several members of Equifax's Vulnerability Assessment Team received the U.S. CERT alert. Once received by Equifax, the alert was forwarded to a distribution list of roughly 400 people within Equifax.

7. What steps did the company take after receiving the US-CERT notification? Please respond in detail and describe every action that was taken, the date on which the action was taken, who took the action, and who in the company each person involved directly reported to.

Response: The Equifax security team took immediate action upon being notified of a potential vulnerability on March 8, 2017. The breach occurred because of both human error and technology failures, not because Equifax failed to take these issues seriously.

On March 9, 2017, Equifax disseminated the U.S. CERT notification internally by email to more than 400 employees, requesting that personnel responsible for an Apache Struts installation immediately upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48-hour time period. Equifax now knows that the vulnerable version of Apache Struts existed within Equifax but was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 14, 2017, Equifax Security implemented rules on its intrusion detection and intrusion prevention devices to detect and block attempts to exploit the Struts 2 vulnerability. These devices successfully identified and blocked a significant number of exploit attempts following implementation.

On March 15, 2017, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. The scans, however, did not identify the Apache Struts vulnerability. Unfortunately, Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability.

8. In your testimony before the House Energy and Commerce Committee on October 3, 2017, you stated that the attack was made possible because of a human error. Please explain in detail what the error was, the position held by the person who committed the error, who in the company this person directly reported to, and which of the individuals involved were part of the company's 225 cybersecurity professionals.

Response: Please see the response to Question 7. At the time the breach was discovered, David Webb was Equifax's Chief Information Officer, Susan Mauldin was Equifax's Chief Security Officer, and Richard Smith was Equifax's CEO. The individual who oversaw the team responsible for patching the relevant Apache Struts vulnerability on software supporting Equifax's online disputes portal reported to Mr. Webb. Both Mr. Webb and Ms. Mauldin retired from their positions, effective September 15, 2017, and Mr. Smith stepped down as CEO on September 25, 2017**.**

9. On March 8, 2017, did Equifax have any protocols for responding to vulnerability notification from US-CERT and what actions should take place following a notification? If so, please explain the protocols in detail, including each task that was required to be completed, who was required to complete the task, who in the company these individual(s) had to directly report to, and any verification mechanisms that were supposed to be in place to check whether each task was completed. Please indicate what, if any, industry standards, guidelines, or best practices were used to develop these protocols.

Response: Please see response to Question 7.

10. What steps has the company taken to address previous error regarding its patching process and to mitigate potential errors in the future?

Response: Equifax has implemented several updates to protocols and procedures in response to this incident. Equifax has made changes to the process by which the Security Global Threat and Vulnerability Management ("GTVM") team notifies the IT team of necessary security patches and system vulnerabilities. The Company is now performing external scans using the Rapid 7 scanner from vendor Nexpose. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company also has implemented additional network, application, database, and system-level logging.

Equifax's forensic consultants have recommended and have implemented a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also retired from their positions.

11. In your testimony before the House Energy and Commerce Committee on October 3, 2017, you stated that a scanner failed to detect a vulnerability in the dispute portal. What scanning technology was your company using to scan this portal? Please respond in detail and include the name of the vendor, software, and service offering if applicable.

Response: Please see response to Question 7. Equifax was using the McAfee Vulnerability Management ("MVM") scanner.

12. When did Equifax begin using this particular vendor and software to scan the dispute portal? Is the company still using the vendor and software to scan this portal?

Response: External scans are now being performed using the Rapid 7 scanner from vendor Nexpose.

13. Who at Equifax conducted the scans on March 15, 2017 and who did the individual(s) directly report to in the company?

Response: Please see response to Questions 7 and 8.

14. How frequently does Equifax conduct vulnerability scans of its dispute portal?

Response: Today, the Company performs weekly full scans of the dispute portal. Additionally, partial scans of the portal are performed daily.

15. What circumstances dictate whether a scan of the dispute portal is conducted?

Response: Please see response to McNerney Question 14.

16. How many scans were conducted of the dispute portal between March 8, 2017 and July 29, 2017? Please provide a list of the dates on which the scans were conducted.

Response: Between March 8, 2017 and July 29, 2017, the dispute portal was scanned 26 times.

1. March 8, 2017
2. March 15, 2017
3. March 19, 2017
4. March 22, 2017
5. March 29, 2017
6. April 5, 2017
7. April 12, 2017
8. April 19, 2017
9. April 23, 2017
10. April 26, 2017
11. May 3, 2017
12. May 10, 2017
13. May 17, 2017
14. May 21, 2017
15. May 24, 2017
16. May 31, 2017
17. June 7, 2017
18. June 14, 2017
19. June 18, 2017
20. June 21, 2017
21. June 28, 2017
22. July 5, 2017
23. July 12, 2017
24. July 19, 2017
25. July 23, 2017
26. July 26, 2017

17. Between March 8, 2017 and July 29, 2017, was any other scanning technology used to scan the dispute portal for potential vulnerabilities besides the scanning technology that was used on March 15, 2017? If so, please list the vendor, software, and service offering if applicable.

Response: Between March 8, 2017 and July 29, 2017, Equifax used McAfee's Vulnerability Manager scanner as its primary scanning technology for vulnerabilities. The company also used Fortify on Demand during software development to scan its source code for potential vulnerabilities.

18. Did Equifax experience any problems with the scanning technology that was used on March 15, 2017 prior to this date?

Response: Equifax is not aware of any problems with the scanning technology that would have caused it to believe that the technology would not identify the Struts vulnerability announced on March 8, 2017 (CVE-2017-5638).

19. Is the scanning technology that was used to conduct the scans on March 15, 2017 used to scan any of Equifax's other portals? If so, please specify the names of the portals.

Response: Equifax used the McAfee Vulnerability Manager to scan all hosts known to Equifax Security, including applications running on those hosts.

20. What type of training on using scanning technology does Equifax provide to the individuals who conduct the vulnerability scans? How many individuals who conduct the scans in the company receive this training? Does the company consider these individuals to be a part of its 225 cybersecurity professionals?

Response: Equifax security professionals responsible for operating the scanners – who are among the Company's cybersecurity professionals – are trained through on-site training provided by the Company's vendors and/or on the job training. Generally, the Equifax employees who are responsible for engineering, deploying, and operating the company's scanning technology participate in training.

21. On March 15, 2015, did Equifax have any protocols in place for conducting vulnerability scans or for measuring the effectiveness of the scans? What, if any, industry standards, guidelines, or best practices were used to develop these protocols?

Response: Equifax produced a copy of the Patch Management Policy (EFXCONG-EC000001341 to EFXCONG-EC000001351) to the Subcommittee on January 26, 2018. That policy outlines the protocols for conducting vulnerability scans.

On March 15, 2017, Equifax had protocols in place regarding conducting and measuring the effectiveness of vulnerability scanning. We are providing two relevant procedure documents. First, the "PCI 11.2 Vulnerability Management Procedures" outlines the vulnerability management procedures. It contemplates monthly assessments to identify, report, and remediate vulnerabilities. It also contemplates using ad-hoc or monthly re-scans to confirm the effectiveness of remediation. The "VMS Detailed Tasks" provides Equifax Security personnel with detailed step-by-step procedures to carry out various scanning tasks, such as scheduling scans, running scans, generating reports, and gathering scanning metrics. Running regular scans, particularly relating to the external network perimeter, is considered an industry best practice, as is the use of rescanning reports to confirm that identified vulnerabilities were remediated.

Copies of the "PCI 11.2 Vulnerability Management Procedures" and "VMS Detailed Tasks" have been provided with this submission and Bates-numbered EFXCONG-EC000002454 to EFXCONG-EC000002477 on the enclosed CD.

22. On March 15, 2017, what were Equifax's internal reporting requirements following vulnerability scans of its portals? What, if any, industry standards, guidelines, or best practices were used to develop these requirements?

Response: Equifax produced a copy of the Patch Management Policy (EFXCONG-EC000001341 to EFXCONG-EC000001351) to the Subcommittee on January 26, 2018. That policy outlines the company's internal reporting requirements following vulnerability scans of its portals.

Equifax's PCI 11.2 Vulnerability Management Procedures, in place on March 15, 2017, specifies, "After a scan is complete, a scan report is produced. This report lists all open vulnerabilities per risk, highlighting the new vulnerabilities. It also lists the vulnerabilities that were closed from the previous scan. This scan report is sent by email to the system custodians." The PCI 11.2 Vulnerability Management Procedures also set forth a process for escalation in the event that vulnerabilities are not remediated in a timely fashion. Having a process for reporting and escalating issues regarding identified vulnerabilities is considered an industry best practice.

23. Since discovering the cyberattack, has the company made any changes with respect to how it conducts vulnerability scans and what technology it uses, particularly as it relates to the dispute portal and any other portals that contain consumer data?

Response: Please see response to Question 10.

24. ls Equifax a member of or does it participate in any of the Department of Homeland Security Sector Coordinating Councils? If not, do you believe that companies such as Equifax could benefit from participating in such efforts?

Response: Yes, Equifax is a member of and participates in the Department of Homeland Security Financial Services Sector Coordinating Council.