GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

October 19, 2017

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

Dear Mr. Smith,

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

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

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

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

Sincerely,

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

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

Additional Questions for the Record

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?

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."[1]

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

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

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

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

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

3. According to a Bloomberg Businessweek investigation, reportedly "there [were] signs that Smith and others were aware something far more serious was going on. The investigation in March was described internally as 'a top-secret project' and one that Smith was overseeing personally."[2] 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.

---

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

[2] Id.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Honorable Brett Guthrie

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

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

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

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

The Honorable David B. McKinley

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

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

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

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

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

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

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

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

The Honorable Markwayne Mullin

1. At least 1.7 million Oklahomans are impacted by this serious breach. I hope they do not experience any incidents of fraud or identity theft as a result, but I imagine some may. Did Equifax have a breach response plan in place before the event that outlined steps the company should take to protect consumers in the event of a date breach?

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

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

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

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

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

The Honorable Jan Schakowsky

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

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

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

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

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

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

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

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

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

iii. Please detail with specificity the differences between the new free credit lock tool that Equifax will begin offering in January and a credit freeze. Include in your response how the tools differ with respect to the consumer experience as well as how the tools differ with respect to the costs, benefits, duties, and rights (both contractual and statutory) for Equifax.

iv. In the FAQs on equifaxsecurity2017.com, Equifax states:

> *-Security freezes were created in the early 2000's, are subject to regulation by each state and use a PIN based system for authentication.*
>
> *-Credit file locks were created more recently, are mobile-enabled and use modern authentication techniques, such as username and passwords and one-time passcodes for better user experience.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. A patch for the vulnerability that 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    a. What specific information and advice did you receive from Mandiant at that time? Did you personally get the warning? Who else in the company received that warning?

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

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

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

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

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

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

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

    a. Do you and Equifax deny that assertion?

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

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

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

    b. What preparations were made for those attacks? Were those preparations completed before public notice occurred on September 7?

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

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

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

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

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

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

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

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

The Honorable Ben Ray Lujan

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

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

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

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

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

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

2. After offering initial resistance to credit freezes, Equifax has made credit freezes or "credit locks" free for one year.

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

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

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

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

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

3. During the hearing, you asserted that from a customer perspective, a credit lock and credit freeze are the same.

    a. If a credit lock and freeze are the same, why doesn't Equifax simply offer credit freezes, which come with strong, well-understood legal protections for consumers, for free?

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

The Honorable John Sarbanes

1. Can minors have their identity stolen?

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

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

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

The Honorable Jerry McNerney

1. Please provide in detail the organizational structure both prior to and after July 29, 2017 of Equifax's Security Department and its Information Technology Department.
2. What function(s) does the Security Department carry out in the vulnerability patching process?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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