

October 12, 2017

Richard F. Smith
Former Chairman and Chief Executive Officer
Equifax
1550 Peachtree St. NE
Atlanta, GA 30309


Dear Mr. Smith:

I remain extraordinarily concerned about the recent cybersecurity breach at Equifax that exposed the personal data of over 145 million Americans. Investigations conducted since that breach revealed extensive problems with the company's efforts at preventing hacking, and with the response by Equifax after the hack was discovered. They reveal a broken industry model in which Equifax and other credit reporting agencies make millions of dollars off of obtaining and trading in customer data – despite never obtaining explicit consent to use it, and having little incentive to adequately protect this data from hackers.

I wrote to you on September 15, 2017, with sixteen questions about the breach and its aftermath,¹ as part of a broad investigation of the breach and the credit reporting industry that I am conducting. I sent you a series of questions the day before the last week's Senate Banking Committee hearing on the Equifax breach.² And I had the opportunity to question you during that hearing.

I appreciate your response to my September 15th letter, and your willingness to attend the Committee hearing. However, I still have numerous questions about the Equifax breach, the company's failure to prevent it, and the company's decisions in the aftermath of the breach. I therefore request that you respond to the following questions – which I have also submitted as Questions for the Record in conjunction with the recent hearing – by November 1, 2017.

Sincerely,



Elizabeth Warren
U.S. Senator

¹ Letter to Richard Smith (Sept. 15, 2017) (available at https://www.warren.senate.gov/files/documents/2017_09_15_equifax.pdf).

² "In Advance of Banking Committee Hearing, Senator Warren Seeks Answers from Equifax's Former and Interim CEOs," (Oct. 3, 2017) (available at https://www.warren.senate.gov/?p=press_release&id=1923).

Extent of the Breach

Despite the fact that Equifax has now known of this breach for over two months, the company has not provided a full and complete accounting of the extent of the breach. Your testimony and your responses to my September 15 letter, while providing some information, failed to answer important questions regarding the precise details and extent of the breach.

For example, you submitted a statement to the Senate Banking Committee that claimed the breach “impacted personal information relating to 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.”³ Not only has Equifax failed to clarify the extent of this impact, but the company has since revised those numbers upwards, announcing that 2.5 million more accounts had been “impacted” than previously publicized. And the company has not offered clear details of how this breach will impact consumers.

- 1. What was the precise extent of the breach?**
 - a. How many U.S. individuals' Social Security numbers were accessed?**
 - b. How many U.S. individuals' birth dates were accessed?**
 - c. How many U.S. individuals' driver's license numbers were accessed?**
 - d. Were Individual Tax Identification Numbers (ITIN) part of the data stolen as part of the breach? If so, how many U.S. individuals' ITINs were accessed?**
 - e. Your press release indicates that “certain dispute documents with personal identifying information” were accessed for 182,000 U.S. customers. Exactly what kinds of documents were accessed?**
 - f. Were any other kinds of document or information accessed besides names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and “certain dispute documents”? If yes, what type of documents, and how many U.S. consumers were affected?**
- 2. What does Equifax mean when the company says that “the incident potentially impacts” personal information? Was information merely exposed to hackers, or were hackers able to exploit and exfiltrate any personal information?**
- 3. What Equifax subsidiaries were affected?**
- 4. Has the company identified the hackers? Is there reason to believe that they are State actors?**

³ “Prepared Testimony of Richard F. Smith,” *Senate Banking Committee* (Oct. 4, 2017) (available at <https://www.banking.senate.gov/public/cache/files/da2d3277-d6f4-493a-ad88-c809781f7011/F143CC8431E6CD31C86ADB64041FB31B.smith-testimony-10-4-17.pdf>).

Equifax's Failure to Protect Consumer Information

At your hearing, you stated that the hack was the result of both human and technological errors. You failed to describe in detail how these errors occurred or what safeguards, if any, Equifax had in place to prevent or mitigate such errors.

I have consulted with numerous cybersecurity experts in the weeks since the breach was made public, and they have raised important questions about additional vulnerabilities that allowed the hackers to access personal data after they entered the system via the Apache Struts vulnerability. These experts indicated that there are two possible ways that this access could have occurred: either Equifax held the sensitive data on an internet-accessible database that hackers accessed through the Apache Struts vulnerability, or the hackers were able to take advantage of other cybersecurity weaknesses to access another corporate network. Either way, this would reveal is an additional failure above and beyond the Apache Struts vulnerability.

- 1. How, precisely, was the personal data that was exposed to the hackers stored and protected? Was this data stored on an internet-accessible outward-facing database?**
- 2. Was the personal information of millions of Americans encrypted in any way? If not, has Equifax begun to use encryption in light of the recent breach?**
- 3. Did the hackers access the data directly via the Apache Struts vulnerability, or were the hackers able to jump from the initial breached system to the corporate network to get that information? If so, how did this occur?**

Equifax has indicated that “[t]he attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.”⁴ But according to the company, “[t]he particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017.”⁵ At your recent hearing, you reiterated that Equifax initiated the proper procedures to patch the vulnerability, but that human error resulted in the failure to fix a known problem. This failure by Equifax to close a known vulnerability in security is deeply troubling, and raises a number of important questions:

- 1. What steps did Equifax take to patch Apache Struts beginning in March 2017? Please provide a detailed timeline of all work on this patch from March 2017 to the present.**
- 2. Your testimony states that Equifax's security department “required that patching occur” within 48 hours. What did Equifax do to require patching?**

⁴ Equifax, Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes (Sept. 15, 2017) (<https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>).

⁵ *Id.*

- a. Did executives follow up with system users in the following weeks to ensure that the patching had occurred?
 - b. Did Equifax monitor its systems to ensure that patching had occurred?
 - c. Did Equifax do anything besides contact system users as part of its efforts to “require” patching of the Apache Struts vulnerability?
3. What safeguards did Equifax have in place to protect against vulnerabilities in the event that all users did not immediately patch an identified weakness? What safeguards has Equifax put in place since this breach?
4. How have Equifax’s protocols and procedures for responding to an identified vulnerability changed since this breach?
5. Which executive in the company was responsible for ensuring that this patch was successfully installed?
6. Was the Apache Struts weakness the only vulnerability that was exploited by the hackers, or has Equifax identified any other weaknesses or vulnerabilities in your cybersecurity system? If so, what were these vulnerabilities and have they been resolved?

In your testimony, you also explained that “scans that should have identified any systems that were vulnerable to the Apache Struts issue” failed to identify the continuing vulnerability nearly a week after your initial internal notification.

1. Has Equifax investigated why and how these scans failed to identify the continuing vulnerability? If so, what has the investigation determined?
2. What software do you use for these scans? Have you updated, upgraded, or replaced this software?
3. Has Equifax performed a full evaluation of its security department to determine whether this and other automated security measures are fully functioning?
4. Did Equifax have safeguards in place to prevent against catastrophic consequences in the event of a failed scan? If not, has Equifax put such measures in place since the breach occurred?
5. How have Equifax’s protocols and procedures for running scans to determine if a vulnerability has been patched changed since the breach?

Equifax’s Initial Response

According to your testimony, Equifax’s security department first observed suspicious network traffic on July 29th, and you were “told about the suspicious activity” on July 30th. Equifax did not notify consumers until a public announcement on September 7th, 40 days after the initial discovery. While you provided the Senate Banking Committee with some information regarding the timeline of events between July 29th and September 7th, a great deal still remains unknown

regarding the actions Equifax took – and more importantly, the actions your former company did not take – during that period.

- 1. Did Equifax consider notifying consumers of a potential breach of their personal information before September 7th?**
- 2. Why did Equifax decide not to give consumers an initial disclosure regarding the potential impacts of the breach that would have allowed them to take precautionary measures to protect themselves?**
- 3. More than two months after the breach, Equifax revised the estimated number of individuals impacted from 143 million to 145.5 million. Given that 40 days elapsed between the discovery of the breach and the initial announcement, how did Equifax miscount the number of affected individuals?**
- 4. Is Equifax confident in the new number, or should consumers expect another recalculation in the future? Where did the 2.5 million new accounts come from?**
- 5. Prior to July 29, 2017 did Equifax have a plan in place to respond to a large-scale security breach?**
 - a. If so, please provide a copy of this plan.**
 - b. If so, was this plan followed in its entirety following the July 2017 breach? If not, where did the Equifax response deviate from this plan, and why?**

Regulatory filings show that three Equifax executives – CFO John Gamble, U.S. Information Solutions President Joseph Loughran, and Workforce Solutions President Rodolfo Ploder – sold stock in the company on August 1st and 2nd, just days after the initial discovery of the breach. At the recent hearing, you claimed that as far as you knew, these men had no knowledge of the extent of the breach, and that these sales were done as a matter of due course, even being cleared through the Chief Legal Officer. While this breach has put the financial security of hundreds of millions of Americans at risk, it is disconcerting that three executives may have decided to profit off their insider information.

- 1. Were any of the three executives listed above aware of the suspicious activity as of August 1st or 2nd?**
- 2. Was John Kelley, the Chief Legal Officer who approved these sales, aware of the suspicious activity as of August 1st or 2nd?**

In your testimony, you claimed that neither you nor anyone at the company was aware of the severity of the breach in early August. You also noted that Equifax retained the cybersecurity group at the law firm of King & Spalding, hired cybersecurity firm Mandiant to investigate the activity, and contacted the FBI on August 2, 2017.

- 1. Why did Equifax take these actions?**
- 2. In how many instances has Equifax taken any or all of those three actions in response to suspicious activity?**
 - a. Please list all instances in which Equifax has hired Mandiant or a similar cybersecurity firm to investigate suspicious activity.**

- b. Please list all instances in which Equifax has contacted the FBI about suspicious activity.
 - c. Please list all instances in which Equifax has retained the cybersecurity group at the law firm of King & Spalding or the equivalent in response to suspicious activity.
3. Were any of the three executives who sold Equifax stock aware of plans or the decision to take any of those three actions?
4. Was Mr. Kelley aware of plans or the decision to take any of those three actions?

Equifax's Post-Breach Efforts for Consumers

In response to the breach, and ostensibly to help consumers determine if their data has been hacked, Equifax created a new website, Equifaxsecurity2017.com. The New York Times reported that, after the website initially went live, consumers were unable to determine with certainty if their information was breached, reporting that the Equifax site for consumers indicated – in response to all inquiries – that personal information “may have” been compromised. As of October 10th, members of my staff were still unable to determine with certainty if their information was compromised.

1. Why was Equifax unable to provide clarity on whether individuals' information was breached?
2. Is there any way for individual consumers to determine with certainty if they were part of the breach? If this cannot be done via the website, how can they determine if this is the case?

Cybersecurity experts consulted by my staff also identified a number of security problems relating to the new website.

3. Does the website run on a stock installation Wordpress? If yes, why did Equifax make the decision to run this installation on this stock installation?
4. Does the Transport Layer Security certificate perform proper revocation checks? What exact checks does it perform? If it does not perform proper revocation checks, why not?
5. Why is the domain name of this website not registered to Equifax?
6. Why does the website provide inaccurate information, informing individuals who enter fake social security numbers that they were part of the breach?
7. Why did Equifax's Twitter account tweet the link to a false domain not owned by Equifax several times? Does Equifax have security measures in place within its digital operations to vet all links sent to consumers?

Equifax initially included a requirement that consumers consent to arbitration in order to determine whether their data had been breached. Equifax also originally required that impacted individuals give their credit card information in order to get one free year of the company's TrustedID Premier credit monitoring and indicated that it would automatically begin billing customers if they did not cancel the subscription within a year.

- 1. Why did Equifax initially include a requirement that consumers consent to arbitration? Did the public outcry against the provision play any role in the decision to remove the arbitration clause?**
- 2. Does Equifax require consumers to consent to arbitration with respect to any of its other products? If so, please provide a list.**
- 3. What is Equifax's justification for including arbitration clauses in some of its consumer contracts?**
- 4. Will Equifax remove arbitration clauses from all consumer contracts?**
- 5. Why did Equifax initially choose to use the auto-billing model for customers?**
- 6. Has Equifax conducted any analyses of how many customers are expected to sign up for the service, and how many are expected to continue receiving the service after twelve months? If so, please provide the results of this analysis.**
- 7. Consumers initially were required to submit sensitive information to TrustedID in order to sign up for credit monitoring. What evaluations has Equifax done of its current data security environment to ensure that the victims of this hack do not, once again, have their information stolen?**

Consumers can protect themselves from fraud by placing a freeze on their credit files. But for nearly a week after it announced the breach, Equifax continued charging consumers for a credit freeze. On September 12th, Equifax announced that it would no longer charge consumers for credit freezes, and would "refund any fees that anyone has paid" since the initial announcement. At your hearing, you explained Equifax's new change, which will extend the availability of free credit freezes through January 2018, and will then transition to a new, free "credit lock" which will be provided to consumers for life.

- 1. Has Equifax provided a full refund to all consumers who paid for a credit freeze after September 7th? If not, has Equifax contacted all consumers who paid for a credit freeze after September 7th regarding a potential refund?**
- 2. How does Equifax's "credit lock" differ from a traditional credit freeze? Please explain in detail how each service works.**
- 3. Will Equifax offer consumers the opportunity to delete their data from Equifax's systems? As of your departure, was Equifax considering this option?**
- 4. Is Equifax considering an "opt-in" regime where consumers would decide whether Equifax should have access to their sensitive personal information in the first place? As of your departure, was Equifax considering this option?**

Equifax Cybersecurity Strategy and Spending

Equifax retains sensitive personal information on millions of customers – and does not rely on explicit consent to obtain and retain this data. Cybersecurity should be a key priority for the company. The latest breach raises important questions about the company’s cybersecurity framework.

- 1. Does the company follow industry best practices? Does the company follow international standards?**
- 2. Who are the company’s five most senior security executives? What are their roles and what are their qualifications?**
- 3. How much did Equifax spend on cybersecurity prevention and preparedness efforts for each of the last five fiscal years? Please provide a broad accounting of these expenditures.**
- 4. Did Equifax consider and reject other cybersecurity strategies? If so, please describe those proposals and the reasoning behind the decision to adopt the current plan.**
- 5. Did Equifax have a detailed breach response plan in place prior to September 2017? If so, what specific steps did this plan entail? Was this plan followed during the response to the most recent breach?**

Experts also indicated that in addition to maintaining all software and application patches, there were two other primary, low-cost security measures that Equifax could and should have taken to reduce the risks and impact of a breach. First, Equifax should have been “logging” all breaches - keeping a record of all breaches and maintaining it in order to quickly catch and address hacks. Second, Equifax should have “locked down” all user credentials. If Equifax had done so, then anyone who gained access through an Apache Struts vulnerability (or another outward-facing system) would not have the privileges to go any further, such as to a corporate network with sensitive information.

- 1. Did Equifax log all breaches? If so, did this log identify the initial breach?**
- 2. Did Equifax “lock down” all individual credentials? If so, has the company identified how and why this did not prevent the hackers from accessing the personal data belonging to over 140 million Americans?**

Previous Cybersecurity Incidents and Warnings

In the years prior to the most recent and largest information breach, Equifax had multiple episodes where company data was access by hackers - including three incidents in 2016 and

2017. Hackers accessed credit-report data held by Equifax between April 2013 and January 2014; Equifax discovered that it mistakenly exposed consumer data “as a result of a technical error that occurred during a software change” in 2015; a breach compromised information on consumers’ W-2 forms that were stored by Equifax units in 2016 and 2017; and Equifax reported in February 2017 that a “technical issue” compromised credit information of some consumers who used identity-theft protection services from a customer.

- 1. What action did Equifax take in response to each of these breaches?**
- 2. Which executives or employees were held accountable for these four breaches?**
- 3. What caused these breaches? Were any of the vulnerabilities identified in these breaches related to Apache Struts or failure to patch known vulnerabilities in Apache Struts or other web applications?**
- 4. Was the root cause of the breach related in any way to the previous hacks that resulted in the theft of W-2 tax and salary data from Equifax in 2016, or the theft of W-2 tax data from Equifax subsidiary TALX earlier this year?**
- 5. Does Equifax know of any other data breaches it had not reported publicly?**

Press reports since the breach also reveal that numerous independent analyses of Equifax cybersecurity identified important weaknesses. In April 2017 – the month before the breach – Cyence, a cyber-risk analysis firm, “rated the danger of a data breach at Equifax during the next twelve months at 50% It also found the company performed poorly when compared with other financial services companies.”

- 1. Were Equifax cyber security experts aware of the Cyence findings prior to the breach?**
- 2. What specific actions were taken by Equifax in response to the Cyence findings?**

SecurityScorecard, another security monitoring firm, identified the precise weakness that was used by the hackers to breach the Equifax system, reporting that “Equifax used older software — such as the Apache Struts tool kit - and often seemed slow to install patches.”

- 1. Were Equifax cyber security experts aware of the SecurityScorecard findings prior to the breach?**
- 2. What specific actions were taken by Equifax in response to the SecurityScorecard findings?**

A third outside review – by the Fair Isaac Corp. – rated Equifax’s “enterprise security score” based on three elements: hardware, network security, and web services. The score declined from 550 out of 800 at the beginning of the year to 475 in mid-July- when the breach had already occurred. According to reports, “By July, 14 public-facing websites run by Equifax had expired certificates, errors in the chain of certificates, or other web-security issues.”

1. **Does Equifax monitor the Fair Isaac enterprise security score?**
2. **Did Equifax conduct an independent assessment of the reasons for the decline in the score between January and July 2017?**
3. **Were Equifax cyber security experts aware of the decline in Fair Isaac ratings prior to and during the breach?**
4. **What specific actions were taken by Equifax in response to the declining Fair Isaac ratings?**

A *fourth* independent review conducted in 2017 also identified significant problems with Equifax cybersecurity. This report by BitSight Technologies gave a company “an ‘F’ in application security and a ‘D’ for software patching.”

1. **Were Equifax cyber security experts aware of the BitSight findings prior to the breach?**
2. **What specific actions were taken by Equifax in response to the BitSight findings?**

Equifax’s Profits as a Result of the Breach

At your recent hearing, I asked you about the profits that Equifax is earning as a result of the recent breach. If just 1 in 7 consumers opt to sign up for Equifax’s credit monitoring service after their free year expires, Equifax will earn more than \$200 million in revenue. While Equifax is currently offering credit monitoring at no cost, the company is making money through a contract with LifeLock for every customer that LifeLock sells credit monitoring to – and they’ve already seen a ten-fold increase in enrollment since the recent breach was announced. And finally, Equifax makes money by selling protection from identity fraud to businesses and government.

1. **As of the most recent data, how many individuals have signed up for Equifax’s free credit monitoring services?**
2. **Has Equifax estimated how many individuals will renew Equifax’s credit monitoring services after the free year expires? If so, what is that estimate?**
3. **If Equifax has offered similar free trial periods in the past, what percentage of participants has renewed after the free period expires?**
4. **How much revenue does Equifax receive from LifeLock for every consumer who purchases credit monitoring services? How much revenue does Equifax receive from LifeLock or other companies for services related to credit scores, credit freezes, credit monitoring, or other credit-related services?**
5. **Since September 7th, how much has Equifax earned under their contract with LifeLock? How much did Equifax receive during the same calendar period in prior years from the same contract?**

Equifax Contract with the Internal Revenue Service

On September 29th, barely three weeks after the public announcement of the recent breach, the Internal Revenue Service (IRS) awarded Equifax a \$7.25 million sole-source contract “to verify taxpayer identity and to assist in ongoing identity verification and validations needs of the Service.” Taxpayers in Massachusetts and across the country are concerned that the same company that just put their data and financial security at risk will now be responsible for preventing taxpayer fraud.

1. **Has Equifax updated its cybersecurity to ensure that it will be able to fulfill its contract with the IRS without putting taxpayers at risk? Please describe the steps taken by Equifax to boost their security and protect taxpayers.**
2. **Equifax received this sole-source contract after protesting the initial award to another company. After Equifax learned of the massive data breach in late July, did Equifax alert the IRS?**
3. **Did Equifax considering withdrawing its protest and permitting another company to fulfill the contract in light of the recent breach exposing fundamental flaws in its cybersecurity?**
4. **How many other federal contracts for handling sensitive personal information are held by Equifax? What was the value of these contracts for FY2015, FY2016, and FY2017? What is the value of these contracts for FY2018? Please provide a list and a brief summary of these contracts.**
5. **Have cybersecurity breaches affected any of the data held under any of these additional contracts?**