ELIZABETH WARREN
MASSACHUSETTS

COMMITTEES:
BANKING, HOUSING, AND URBAN AFFAIRS
HEALTH, EDUCATION, LABOR, AND PENSIONS
ARMED SERVICES
SPECIAL COMMITTEE ON AGING

United States Senate

UNITED STATES SENATE
WASHINGTON, DC 20510–2105
P: 202–224–4543

2400 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
P: 617–565–3170

1550 MAIN STREET
SUITE 406
SPRINGFIELD, MA 01103
P: 413–788–2690

www.warren.senate.gov

October 3, 2017

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

Paulino de Rego Barros, Jr.
Interim Chief Executive Officer
Equifax
1550 Peachtree St. NE
Atlanta, GA 30309

Dear Mr. Smith and Mr. Rego Barros:

Later this week, the Senate Committee on Banking, Housing, and Urban Affairs will hold a hearing on the recent Equifax data breach. As you know, that breach allowed criminal hackers access to sensitive personal information – including Social Security numbers, birth dates, credit card numbers, and driver's license numbers – for as many as 145.5 million Americans. This breach was inexcusable, as was Equifax's response in the days and weeks after the company learned about the breach and informed the public about it.

In the wake of the breach, I opened a thorough investigation of Equifax, the data breach, and the credit reporting industry as a whole. I sent you a letter on September 15 asking for information on the leak and the response to it. I also sent letters to Experian and Transunion, the two other credit reporting agencies, and to the Consumer Financial Protection Bureau and the Federal Trade Commission about their responses to and their regulatory authority relating to credit reporting agencies and data security breaches.[1]

One week later, I sent additional letters asking for information to the Equifax Board of Directors about potential clawback of executives' pay in response to the breach, to the Department of Homeland Security regarding reports that the vulnerability that lead to the breach

[1] Sen. Elizabeth Warren, Warren Launches Investigation into Equifax Breach with Letters to Equifax, Transunion, Experian, FTC, CFPB, GAO (Sep. 15, 2017) (https://www.warren.senate.gov/?p=press_release&id=1838).

had been reported to Equifax as early as March 2017, and to the Securities and Exchange Commission regarding potentially misleading investor disclosures by Equifax.[2]

The letter that I sent you on September 15 contained sixteen separate questions. I asked for information to address a series of facts that were unclear at the time. I asked about how and when you discovered the breach; precisely how big the breach was and what it entailed; and why Equifax waited 40 days to inform customers of the breach. I asked about whether and how Equifax informed regulators of the breach, and what actions were taken to identify the root cause and make sure that all vulnerabilities were closed. I asked about problems with the Equifax website that was created to help consumers learn about the breach, and about whether Equifax had a plan in place to respond to breaches prior to this incident. And I asked many more questions.

You provided a response to many of these questions on October 1, 2017; this response answered some of my questions in full; it failed to answer others; and in some cases, it raised new questions. In addition to your correspondence, my staff has obtained information from news reports and outside experts that raises additional questions about Equifax and its response to this breach. I am particularly troubled by reports that Equifax had ample warning of cybersecurity problems prior to the 2017 breach, and by reports that the website created to direct consumers to assistance in the wake of the breach – EquifaxSecurity2017.com – also may present a cybersecurity risk.

The remainder of this letter contains my complete set of questions. You will be testifying before the Banking Committee later this week. I ask that you come prepared to answer these and any additional questions that members may have about this betrayal of customer trust and corporate responsibility. I also ask that, following the hearing, you provide full and complete answers to all of these questions for the Committee record.

Questions about the Extent of the Breach

Despite the fact that Equifax has now known of this breach for over nine weeks, and has put out two public statements on the breach, the company has not provided a full and complete accounting of the extent of the breach. For example, describing the extent of the breach, the company initially stated vaguely that "the incident potentially impacts personal information relating to 143 million U.S. consumers – primarily names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

[2] Sen. Elizabeth Warren, Senator Warren Expands Equifax Investigation with Three New Information Requests (Sep. 22, 2017) (https://www.warren.senate.gov/?p=press_release&id=1893).

Equifax also identified unauthorized access to limited personal information for certain U.K. and Canadian residents." The initial Mandiant analysis of the breach provided few additional details on what precisely was exposed, and on whether information was merely "accessed" or whether it was exploited and exfiltrated.[3] But an Equifax release yesterday indicated that "approximately 2.5 million additional U.S. customers were potentially impacted, for a total of 145.5 million."[4]

1. What was the precise and specific extent of the breach?
    a. What does Equifax mean when it says a consumer is "potentially affected"?
    b. How many U.S. individuals' Social Security numbers were accessed?
    c. How many U.S. individuals' birth dates were accessed?
    d. How many U.S. individuals' driver's license numbers were accessed?
    e. Your press release and the Mandiant executive summary indicate that "certain dispute documents with personal identifying information" were accessed for 182,000 U.S. customers. Exactly what kinds of documents were accessed and what kind of personal identifying information was contained in them?
    f. Were any other kinds of documents 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. Initially Equifax stated that "the incident potentially impacts" personal information. The Mandiant Executive Summary notes that "the attacker issued commands to acquire data from numerous tables from numerous database tables." Please clarify: was information merely exposed to hackers, did hackers attempt but not succeed in acquiring and exfiltrating data or were hackers actually able to exploit and exfiltrate personal information?
3. Has the company identified the hackers? Is there reason to believe that they are State actors?

How Did Hackers Gain Access to the Sensitive Information of 145.5 Million People?

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. According to the Mandiant report, "the attackers compromised two systems that support the Online Dispute web application."[5]

---

[3] Mandiant, Executive Summary (Sep. 2017)

[4] Equifax, Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident (Oct. 2, 2017).

[5] Mandiant, Executive Summary (Sep. 2017)

The experts we consulted 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 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?
2. Was this data stored on an internet-accessible outward-facing database?
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?

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. This potential issue appears to be significant because, according to Mandiant, the "attacker accessed files that contained Equifax credentials ...and performed database queries that provided access to documents and sensitive information stored in databases in an Equifax legacy environment."[6]

1. Did Equifax log all breaches and continuously monitor these logs? Did this log identify the initial breach?
2. The Mandiant Executive Summary appears to indicate that a retroactive review of the log was able to identify the breach as occurring on May 13, 2017, but that Equifax did not identify the breach until over two months later.[7] Is this accurate? And if so, why did Equifax not identify the breach when it first occurred?
3. 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?

Equifax Cybersecurity Strategy and Spending

[6] Mandiant, Executive Summary (Sep. 2017)
[7] Mandiant, Executive Summary (Sep. 2017)

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. But it is not clear that this has been the case. The latest breach – and the fact that Equifax was the victim of at least three other breaches since 2016 – 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 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?

Why Did Equifax Ignore Important Warnings and Previous Cybersecurity Incidents?

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.[8]

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?

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."[9]

---

[8] Wall Street Journal, Equifax Security Showed Signs of Trouble Months Before Hack (Sep. 26, 2017) (https://www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947).
[9] Id.

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 were 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." [10]

3. Were Equifax cyber security experts aware of the SecurityScorecard findings prior to the breach?
4. 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.[11] 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." [12]

5. Does Equifax monitor the Fair Isaac enterprise security score?
6. Did Equifax conduct an independent assessment of the reasons for the decline in the score between January and July 2017?
7. Were Equifax cyber security experts aware of the decline in Fair Isaac ratings prior to and during the breach?
8. 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." [13]

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

Questions on Problems with the Equifaxsecurity2017.com Website

---

[10] Id.
[11] Id.
[12] Id.
[13] Id.

In response to the breach, and ostensibly to help consumers determine if their data has been hacked, Equifax created a new website, Equifaxsecurity2017.com. But security experts with whom I have consulted have indicated that the new website has a number of important technical vulnerabilities that could compromise security. Specifically, they noted that the system runs on "a stock installation of Wordpress," which does not provide appropriate enterprise-grade security; that the site does not perform proper revocation checks; and that the domain name itself does not appear to be registered to Equifax.

1. 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. Why was Equifax unable to provide clarity on whether individuals' information was breached?
2. 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?
3. 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?
4. Why is the domain name of this website not registered to Equifax?
5. Why does the website provide inaccurate information, informing individuals who enter fake social security numbers that they were part of the breach?
6. 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?

Questions on the Failure to Patch Key Vulnerabilities

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."[14] But according to the company, "[t]he particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017. Equifax's Security organization was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems in the company's IT infrastructure."

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.

[14] 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).

2. Did Equifax outsource the management of this patch to a third party entity, or was the work conducted in-house?
3. Which executive in the company was responsible for ensuring that this patch was successfully installed?
4. Has Equifax identified why efforts to patch Apache Struts failed? If so, please explain why.
5. 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?

I ask that you come to the hearing on Wednesday prepared to answer these and any other questions that members may have. And I ask that you provide me with full written answers to these questions no later than October 16, 2017.

Sincerely,

Elizabeth Warren
Ranking Member
Senate Subcommittee on Financial Institutions and Consumer Protection