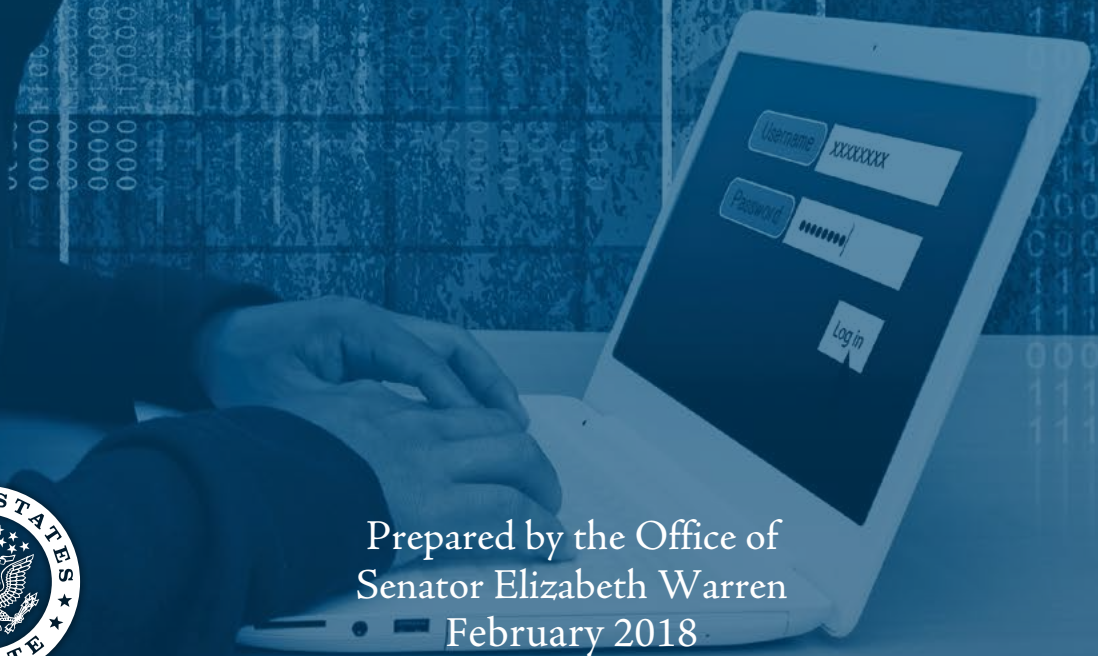
Bad Credit:

UNCOVERING EQUIFAX'S FAILURE TO PROTECT AMERICANS' PERSONAL INFORMATION



Prepared by the Office of
Senator Elizabeth Warren
February 2018

Contents

Executive Summary

Equifax, one of the nation's largest credit reporting agencies, revealed on September 7, 2017, that the company had allowed an extraordinary breach of personal information. Sensitive information belonging to over 145 million Americans was exposed as a result of the breach – one of the largest and most significant data security lapses in history.

One week after Equifax revealed the breach, Senator Elizabeth Warren opened an investigation into the causes, impacts, and response to the exposure of millions of Americans' personal data. She questioned Equifax executives in Senate hearings, consulted outside experts, and sent letters containing dozens of questions to Equifax, to federal regulators, and to other credit rating agencies. The information they provided, and information obtained from additional sources, allowed the staff to reach a series of robust and important findings. This report presents the results of Senators Warren's Equifax investigation. It finds that:

- **Equifax Set up a Flawed System to Prevent and Mitigate Data Security Problems.** The breach was made possible because Equifax adopted weak cybersecurity measures that did not adequately protect consumer data. The company failed to prioritize cybersecurity and failed to follow basic procedures that would have prevented or mitigated the impact of the breach. For example, Equifax was warned of the vulnerability in the web application software Apache Struts that was used to breach its system, and emailed staff to tell them to fix the vulnerability – but then failed to confirm that the fixes were made. Subsequent scans only evaluated part of Equifax's system and failed to identify that the Apache Struts vulnerability had not been remediated.

- **Equifax Ignored Numerous Warnings of Risks to Sensitive Data.** Equifax had ample warning of weaknesses and risks to its systems. Equifax received a specific warning from the Department of Homeland Security about the precise vulnerability that hackers took advantage of to breach the company's systems. The company had been subject to several smaller breaches in the years prior to the massive 2017 breach, and several outside experts identified and reported weaknesses in Equifax's cyber defenses before the breach occurred. But the company failed to heed – or was unable to effectively heed – these warnings.

- **Equifax Failed to Notify Consumers, Investors, and Regulators about the Breach in a Timely and Appropriate Fashion.** The breach occurred on May 13, 2017, and Equifax first observed suspicious signs of a problem on July 29, 2017. But Equifax failed to notify consumers, investors, business partners, and the appropriate regulators until 40 days after the company discovered the breach. By failing to provide adequate information in a timely fashion, Equifax robbed consumers of the ability to take precautionary measures to protect themselves, materially injured investors and withheld market-moving information, and prevented federal and state governments from taking action to mitigate the impacts of the breach.

- **Equifax Took Advantage of Federal Contracting Loopholes and Failed to Adequately Protect Sensitive IRS Taxpayer Data.** Soon after the breach was announced, Equifax and the IRS were engulfed in controversy amid news that the IRS was signing a new $7.2 million contract with the company. Senator Warren's investigation revealed that Equifax used contracting loopholes to force the IRS into signing this "bridge" contract, and the contract was finally cancelled weeks later by the IRS after the agency learned of additional weaknesses in Equifax security that potentially endangered taxpayer data.

- **Equifax's Assistance and Information Provided to Consumers Following the Breach was Inadequate.** Equifax took 40 days to prepare a response for the public before finally announcing the extent of the breach – and even after this delay, the company failed to respond appropriately. Equifax had an inadequate crisis management plan and failed to follow their own procedures for notifying consumers. Consumers who called the Equifax call center had hours-long waits. The website set up by Equifax to assist consumers was initially unable to give individuals clarity other than to tell them that their information "may" have been hacked – and that website had a host of security problems in its own right. Equifax delayed

their public notice in part because the company spent almost two weeks trying to determine precisely which consumers were affected by the breach – but then failed to provide consumers with any specific information to determine if their data was breached. And while Equifax continues to publicly state only that data was "accessed," the company has confirmed that the data was exfiltrated – stolen – from their systems and downloaded by the hackers. Equifax appeared to be more focused on using the breach as a profit-making opportunity for other company services rather than providing redress to consumers.

- **Federal Legislation is Necessary to Prevent and Respond to Future Breaches.** Equifax and other credit reporting agencies collect consumer data without permission, and consumers have no way to prevent their data from being collected and held by the company – which was more focused on its own profits and growth than on protecting the sensitive personal information of millions of consumers. This breach and the response by Equifax illustrate the need for federal legislation that (1) establishes appropriate fines for credit reporting agencies that allow serious cybersecurity breaches on their watches; and (2) empowers the Federal Trade Commission to establish basic standards to ensure that credit reporting agencies are adequately protecting consumer data.

I. INTRODUCTION

On September 7, 2017, the massive credit reporting company Equifax publicly revealed a breach of the company's computer systems – described as "one of the largest risks to personally sensitive information in recent years" – that exposed data from over 145 million Americans to criminal hackers.[1] The company indicated that a vast trove of sensitive data – including social security numbers, credit card numbers, passport numbers, and driver's license numbers – may have been compromised. The incident was the fifth recent data breach of Equifax or its subsidiaries that endangered American's personal information.[2]

A subsequent internal investigation released by Equifax revealed additional information: that the company first became aware of the breach in July 2017; that the first breach occurred months earlier, in May 2017; and that the cause of the breach was a vulnerability in a web-application software, Apache Struts, that was used by Equifax and many other companies.[3]

Equifax announced a series of actions when the company publicly revealed the breach or soon thereafter, including monitoring of consumer credit files; the ability to access, review, and lock Equifax credit files; an insurance policy that covers out-of-pocket expenses stemming from identity theft; and ongoing review for misuse of consumers' social security numbers.[4] The company also announced on September 15, 2017, that two top executives responsible for the company's cybersecurity were immediately "retiring,"[5] and on September 26, 2017, announced the retirement of CEO Richard F. Smith.

Consumer concerns about the Equifax breach were particularly stark because the company – along with the two other large credit reporting agencies, Experian and TransUnion – occupy a unique place in the financial world: they obtain and use massive amounts of data on millions of consumers, but consumers have little to no power over how this data is collected, how it is used, or how it is kept safe.

As a result of these concerns, Senator Warren opened an investigation into the causes of, response to, and impact of the Equifax data breach. She sent several letters to Equifax seeking information; she questioned the former Equifax CEO in a Senate hearing; she wrote to Experian and TransUnion seeking information on their cybersecurity practices; she wrote to federal regulators seeking information on their authority to prevent and respond to cybersecurity breaches; she wrote to the Internal Revenue Service with Senator Ben Sasse to get information and answers surrounding the agency's decision to award a contract to Equifax to verify taxpayer identities; her staff reviewed internal investigations of the Equifax breach conducted by the cybersecurity firm Mandiant; and her staff consulted with independent cybersecurity experts.[6] This report presents the results of Senator Warren's detailed investigation of the Equifax cybersecurity breach.

II. FINDINGS

A. Equifax Failed to Take Adequate Steps to Prevent the Data Breach

1. Equifax Set up a Flawed System to Prevent and Mitigate Data Security Problems

This investigation finds that the breach was made possible because Equifax adopted weak cybersecurity measures that failed to protect consumer data – a symptom of what appeared to be the low priority afforded cybersecurity by company leaders. The CEO at the time of the breach, Richard Smith, testified that despite record profits in recent years, Equifax spent only a fraction of its budget on cybersecurity – approximately 3 percent of its operating revenue over the last three years.[7] In contrast, Equifax paid nearly twice as much in dividends to shareholders.[8]

Cybersecurity experts consulted by Senator Warren staff indicated that a large company that holds sensitive data, such as Equifax, should have multiple layers of cybersecurity. Equifax should have had (1) frequently updated tools to prevent hackers from breaching their systems; (2) controls that limited hackers' ability to move throughout their systems in the event of an initial breach; (3) restrictions on hackers' ability to access sensitive data in the event of an initial breach; and (4) procedures to monitor and log all unauthorized access in order to stop the intrusion as quickly as possible. Despite collecting data on hundreds of millions of Americans without their permission, Equifax failed to fully and effectively adopt any of these four security measures.

This investigation identified the following weaknesses in Equifax's cybersecurity:

- **Faulty Patch Management Procedures:** For many vulnerabilities that arise in its software and applications, Equifax only has to deploy a software "patch" that will fix the vulnerability and restrict access to the susceptible system. It's like putting a Band-Aid on a cut – simple, effective, and cheap. Yet Equifax let numerous software vulnerabilities sit un-patched for months at a time, leaving weaknesses through which hackers could gain access.[9] The failure to fully deploy a free Apache Struts patch led directly to the breach that compromised the data of millions of Americans.[10] Equifax failed to effectively use these simple, low-cost patches to protect consumer data.[11] In a briefing provided to Banking Committee staff, Equifax explained how this happened: they were warned of the vulnerability, and emailed staff to fix it.[12] But not all staff received this email, meaning not all necessary updates were in place – and Equifax failed to perform appropriate checks that would have identified this egregious error.[13] A subsequent security scan only covered part of Equifax's system, missing that the Apache Struts vulnerability was still present.[14]

- **Feeble Monitoring of Endpoint and Email Security:** Hackers often exploit weaknesses in the security of individual users of a system – for example, with spear phishing attacks over e-mail. In order to detect attacks on its system, Equifax must monitor laptops and other network devices that have access to its systems. But Equifax failed to adopt strict endpoint and email security measures.[15] While Equifax has now indicated that they are making improvements to their cybersecurity measures, it is too late to prevent the breach that put over 145 million Americans at risk.

- **Exposure of Sensitive Information:** In addition to adopting weak external security measures that allowed hackers to breach its systems, Equifax also failed to effectively secure sensitive consumer information.[16] When a bank locks its doors at night, it doesn't leave the money on the front counter in the assumption that nobody will break in. It locks the cash in the vault. Equifax, on the other hand, retained sensitive consumer information on easily accessible systems. Once the hackers exploited the Apache Struts vulnerability and gained access to Equifax's system, they found a treasure trove of consumer information at their fingertips.

- **Weak Network Segmentation:** Equifax also failed to put security measures in place that would prevent hackers from jumping from insecure, internet-facing systems to backend databases that contain more valuable data.[17] In other words, putting your valuables in a vault doesn't do much good if you forget to lock it. Equifax's network

segmentation measures failed to keep hackers from accessing consumer information because the company did not adopt adequately strict measures to protect valuable data.[18]

- **Inadequate Credentialing:** Equifax's cybersecurity failures extended to their internal security. Each user on Equifax's system receives a set of privileges. Under a strict security standard, Equifax would limit access to the most critical databases to just a handful of necessary users. This would protect the company from internal attacks and further bolster the company's overall data security regime. After gaining access to Equifax's system, hackers then acquired user credentials – a username and password – and accessed a huge quantity of sensitive information using just those credentials.[19] The company did not adopt adequately strict security measures to properly restrict user access to sensitive data.[20]

- **Logging:** Equifax neglected the use of robust logging techniques that could have allowed the company to expel the hackers from their systems and limited the size and scope of the data breach.[21] Logging is a simple but crucial cybersecurity technique in which companies monitor their systems, continuously logging network access in order to identify unauthorized users. Logging cannot necessarily prevent a breach, but just as a security camera can monitor access to a bank and allow a quick response when a break-in is identified, a robust monitoring system can identify and catch a hacker more quickly, allowing security to shut down the system and prevent future access. Equifax allowed hackers to continuously access sensitive data for over 75 days, in part because the company failed to adopt effective logging techniques and other security measures.[22]

Equifax was making huge profits but failing to protect consumers' data safety and security. Equifax adopted ineffective cybersecurity measures for sensitive data belonging to millions of Americans. As a company that has "data on approaching a billion people," and "manage[s] massive amounts of very unique data," as CEO Rick Smith put it two weeks after learning of the breach, Equifax failed to take the necessary efforts to protect that data.[23] While Equifax has found no evidence that this information has been sold, their actions put millions at risk of identity theft for the rest of their lives.[24] Equifax's goal, as stated by its CEO just weeks before he disclosed the breach, was to go from "$4 billion in revenue to $8 billion" in approximately 5 years.[25] Equifax prioritized growth and profits – but did not appear to prioritize cybersecurity.

2. Equifax Ignored Numerous Warnings of Risks to Sensitive Data

The Equifax data breach did not come out of the blue. The company had ample warning of potential risks to its systems and potential weaknesses. Equifax was subject to several smaller breaches in the years prior to the massive 2017 breach and received a specific warning from the Department of Homeland Security about the Apache Struts vulnerability that was used by the hackers to breach the company's systems. But Equifax failed to heed – or was unable to effectively heed – these warnings.

Equifax received the first notification of the Apache Struts vulnerability via a specific warning from the Department of Homeland Security U.S. Computer Emergency Readiness Team (CERT) on March 8, 2017.[26] Richard F. Smith, former Equifax CEO, testified that the company disseminated the U.S. CERT warning the next day, "requesting that applicable personnel… upgrade their software… within a 48 hour time period."[27] One week later, the company ran a series of internal scans that "should have identified any systems that were vulnerable" to that weakness.[28] These scans did not reveal any problems. The unpatched vulnerability remained for two months, until hackers used it to breach Equifax's network on May 13.[29] Equifax later admitted that the company failed to close the loop and confirm whether the fixes were made, and revealed that the subsequent scans only evaluated part of Equifax's systems.[30]

Equifax had other warnings of potential problems. Prior to the breach revealed in September 2017, there were four different instances when company data was accessed by hackers between 2013 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."[31]

Press reports also revealed that four independent analyses of Equifax cybersecurity, conducted either before or immediately after the breach, identified important weaknesses.

(1) 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 12 months at 50%. It also found the company performed poorly when compared with other financial-services companies."[32]

(2) 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."[33]

(3) An 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."[34]

(4) A fourth independent review released just after the breach was revealed identified significant problems with Equifax cybersecurity. This report by BitSight Technologies gave the company an "'F' in application security and a 'D' for software patching."[35]

B. Equifax Failed to Notify Consumers, Investors, and Regulators about the Breach in a Timely and Appropriate Fashion

Equifax was first warned about the vulnerability that led to the breach on March 8, 2017; the breach occurred on May 13, 2017, and Equifax first observed suspicious network traffic on July 29; Equifax's CEO first learned of the suspicious activity on July 31; and Equifax engaged a cybersecurity consulting firm, retained a law firm, and contacted the Federal Bureau of Investigation on August 2.[36] Equifax knew of the major breach, and knew it was significant, but spent almost two weeks trying to identify precisely which customers were affected – all while saying nothing to regulators or the public.[37] By August 11, Equifax knew that hackers likely accessed "a database table containing a large amount of consumers' PII.[38]" Equifax failed to notify consumers, investors, business partners, and other regulators until September 7, 40 days after the company initially discovered the breach.[39]

In addition, Equifax has publicly stated on numerous occasions that data was "accessed" – leaving it unclear if hackers merely obtained access to, or actually stole the data. But in a December 11 Banking Committee staff briefing, Equifax officials confirmed that, in fact, data tables were "exfiltrated" – stolen – by the hackers.[40]

By failing to provide adequate information about the breach – either publicly, or privately to regulators and other business partners – Equifax robbed consumers of the ability to take precautionary measures to protect themselves; materially injured investors and withheld market-moving information; and prevented the federal government from taking action to remedy the situation and cut ties with Equifax in other contracts. Equifax failed to notify the following parties in a timely fashion:

- **Consumers:** Equifax exposed the sensitive personal information of over 145 million individuals, yet the hackers that stole this information had more than a month to take advantage of consumers who had no idea they were at risk. Equifax did not give consumers a chance to obtain credit freezes, cancel their credit cards, place fraud alerts or credit monitoring on their accounts, or take any number of precautionary measures to ensure their financial safety. Furthermore, Equifax failed to disclose the fact that the hackers gained access to consumers' passport numbers.[41] And four months after the breach, Equifax still has not affirmatively notified all individual consumers that were impacted by the breach.[42]

- **Investors:** According to the SEC's cybersecurity guidance, Equifax has a duty to disclose information that a "reasonable investor would consider important to an investment decision."[43] This includes "costs or other consequences" of a breach, including the potential costs of remediation, protection, lost revenues, and reputational harm.[44] After first learning of suspicious activity on its network, Equifax waited 40 days to inform investors – filing an 8-K form with the SEC on the same day it made a public announcement.[45] And Equifax missed other key opportunities to inform investors of risks.

  In particular, Equifax held an investor presentation on August 16, more than two weeks after the initial discovery and one day after Equifax CEO Rick Smith learned that consumer personally identifiable information had been stolen in the breach.[46] Equifax neglected their duty to investors by failing to inform them of the breach during that presentation, and continued to withhold material information that had a large impact on the company for more than three weeks.

- **Government Regulators:** The Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) regulate Equifax. The FTC has primary authority to enforce the Gramm-Leach Bliley Act, which provides data security requirements for non-bank financial institutions. The FTC and the CFPB have concurrent authority to enforce the Fair Credit Reporting Act, which requires credit reporting agencies to maintain "reasonable procedures" to protect consumer data, but are not specifically designed to address cybersecurity threats.[47] And while the FTC can bring lawsuits against companies that have allowed data to be compromised, the agency does not have authority to provide ongoing supervision of company practices.[48] The Department of Homeland Security also addresses cybersecurity threats, and warned Equifax about the vulnerability that hackers eventually utilized to breach the company's networks and access consumer data. Yet Equifax failed to notify its regulators for more than a month after first learning of suspicious activity, leaving them behind the curve in helping consumers deal with the consequences. The FTC, the CFPB, and DHS only learned of the breach when it was disclosed to the public.[49]

  The FTC was forced to hastily address the regulatory and public interest concerns rather than having time to prepare a response. The FTC released an advisory to consumers after Equifax's public announcement of the breach that eventually became the most viewed webpage in the federal government.[50] If Equifax had informed the agency sooner, the FTC could have worked to make sure consumers were prepared and protected, and advised them immediately following Equifax's announcement.

  Equifax also failed to inform state agencies and Attorneys General of the breach, delaying action at the state level under appropriate state laws.[51]

- **Federal Contractors:** Equifax also failed to inform government agencies with which the company holds federal contracts of the breach. For example, Equifax did not notify the IRS of its data breach for 40 days after first learning of suspicious activity.[52] Although reviews conducted by the IRS after the breach indicated that there was no consumer tax data exposed to hackers, Equifax's delay potentially placed this data at risk.

C. Equifax took advantage of federal contracting loopholes and failed to maintain adequate protections for sensitive IRS taxpayer data

Over the last decade, Equifax has been awarded 2,106 Federal contracts worth over $120 million.[53] These contracts have been awarded by dozens of agencies, including the General Services Administration, the Department of Justice, the Department of Homeland Security and the Equal Employment Opportunity Commission.[54]

Equifax was involved in the exposure of consumer data in several instances while it was performing Federal contracts. In some cases, these contracts involved particularly sensitive personal information. For example, in 2013, the Center for Medicare and Medicaid services awarded a five year, $329 million contract to Equifax to verify income and employment information for Americans who applied for subsidies under the Affordable Care Act.[55]

A recent controversial contract was awarded to Equifax in 2015[56] by the Internal Revenue Service (IRS) to verify taxpayers' identities in an online portal that allows taxpayers access to their tax documents.[57] This contract – and the IRS – became the subject of intense criticism when it was announced that it would be renewed soon after Equifax revealed the breach in September 2017.[58] Several weeks later, the IRS reversed itself and suspended the contract on October 12, 2017.[59]

This investigation reveals that Equifax used loopholes in Federal procurement law to obtain this extension, gouging taxpayers in the process and placing data at risk. In response to a request, the IRS provided Senator Warren's staff with a briefing on this matter. In this briefing, staff learned that the IRS suspended this contract after the agency learned of a number of additional flaws in how Equifax was handling sensitive taxpayer data.[60]

In June 2017, the IRS asked companies to bid for a contract to verify taxpayers' identities on its online portal.[61] Equifax had won the previous contract in 2015 and bid again, but Experian underbid Equifax, asking for less than a third of Equifax's bid – a savings of more than $1.7 million in taxpayer dollars to provide the same services.[62] But barely a week after the contract was awarded to Experian in late June, Equifax protested the award.[63] Federal procurement law gives the Government Accountability Office 100 days to resolve the dispute.[64] Even after it announced the massive security breach, Equifax continued its protest.[65] And because of the protest, the IRS couldn't start the 2-3 month process of integrating Experian into its system as the new contractor.[66]

Because of this delay, the IRS was forced to seek a "bridge contract" to keep the online portal open during the appeal, when victims of Hurricanes Harvey and Maria were relying on the portal to get access to financial documents they had lost. Equifax took advantage of the IRS during this period by raising their price for the bridge contract.[67] In fact, the total bridge contract, which included a three-month contract with two additional three month options, would cost taxpayers $7.3 million – more than nine times as much as Experian will charge for a full year of service ($795,000).[68] This bridge contract was awarded on September 29.[69]

The IRS found out about the breach at the same time as the American public.[70] Within a day, the IRS was on the phone with Equifax, and within two weeks IRS staff was on the ground checking the Equifax systems to make sure no taxpayer information had been compromised.[71] The IRS determined that no data was compromised in this case – but the six-week delay in informing the IRS of the breach could have left taxpayers vulnerable to hackers.[72]

On October 13, a little over one week after announcing the bridge contract, the IRS reversed itself and announced that it was suspending the bridge contract with Equifax.[73] This was because Equifax announced new information that put taxpayer information at risk.[74]

There is no indication that any IRS data was exposed in the breach. But because of the delays, the IRS was forced to give Equifax an expensive bridge contract, and belatedly discovered – weeks after they should have been warned – that Equifax was not able to effectively protect taxpayer data to IRS standards.

D. Equifax's assistance to consumers following the breach was sorely inadequate

On September 7, 2017, when Equifax publicly announced the breach, then-CEO Richard Smith wrote that "[w]e…are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."[75]

But after failing to prevent the breach, the company then failed to effectively respond to it and provide adequate assistance to the millions of Americans put at risk. Equifax did not have an adequate crisis management plan in place, and the company failed to follow the procedures they did have in place for notifying consumers affected by the breach.[76] From the start, the victims of the breach were faced with an obstacle course riddled with traps and frustrations. In fact, as of November 21, 2017, the CFPB handled "over 7,500 complaints" related to the breach, and "a large number of complaints involved specific problems with Equifax's post-breach response."[77] According to the CFPB, "Consumers described difficulty in reaching Equifax's call centers and in accessing their security freeze PIN when adding a freeze online.

Consumers mentioned lengthy hold times, dropped calls, agents not calling back as promised, and call centers that were not helpful."[78] These failures occurred despite the fact that Equifax had 40 days after learning of the breach to prepare their public response.

1. Failure to Adopt or Follow an Effective Breach Response Plan

Equifax confirmed, in response to questions from Senator Warren, that the company has "several plans and procedure guides that address cybersecurity incidents," including the company's Security Incident Handling Procedure Guide, Security Incident Response Team Plan, and Security and Safety Crisis Action Team Plan.[79] While Equifax provided my office with a 150-page Corporate Crisis Management Plan,[80] including a full chapter on Security Incident Handling Policy & Procedures, there are a number of problems with this plan.

The Security Incident procedures are dated October 2014, indicating that they have not been updated in over three years.[81] Moreover, this Crisis Management Plan appears to place little emphasis on protecting the well-being of the millions of individuals whose data are used by Equifax, and often appears more focused on physical security threats and shareholder value [82] than protecting the victims of cybersecurity breaches. For example, the three key overarching principles listed in the Crisis Management Plan are to "Place the highest priority on Life Safety…protect our assets and preserve our ability to operate and supply our customers, [and] maintain a strong Equifax reputation through ethically and socially aware behaviors that ultimately preserve shareholder value." These principles say nothing about protecting sensitive consumer data that earn Equifax hundreds of millions in revenue per year.

The specific "Unauthorized Access Incident Handling Checklist" in the Equifax Security Incident Handling Policy & Procedures does not include informing customers of potential access to their personal data.[83] Instead, these procedures are listed separately in the crisis response handbook – and even then, are not appropriately detailed. For example, there is no clear required deadline or timeline to inform customers about a breach that places their personal data at risk – perhaps explaining why Equifax did not inform the public until over 40 days after the incident.

Finally, it appears that Equifax failed to follow its own procedures for informing the public of breaches. These procedures require that notice be provided to affected customers "in a clear and conspicuous manner, either by telephone or in writing."[84] But according to information provided to Senator Warren's staff, Equifax provided such notice only to 2.5 million affected consumers – the remaining 140 million-plus consumers received notice of the breach only if they went to the company website on their own volition.

2. Problems with the Equifax Call Center

From the start, the Equifax call center had major problems. Consumers sometimes waited up to an hour, if not more, to speak to a representative.[85] Equifax took advantage of the hold time to advertise for various Equifax products.[86] When Equifax representatives eventually got on the phone, they were unable to give consumers even the most basic information about whether their data had been compromised. Callers who wanted to put a fraud alert on or freeze their account were also out of luck – or at least in for a merry-go-round of additional toll-free numbers and dropped calls that even if successful, cost consumers hours of time and aggravation.[87] The CFPB received numerous complaints describing "difficulty in reaching Equifax's call centers and in accessing their security freeze PIN[,]" as well as "lengthy hold times, dropped calls, [and] agents not calling back as promised."[88]

3. Problems with EquifaxSecurity2017.com

Equifax set up a website, EquifaxSecurity2017.com, and instructed consumers to visit to determine whether their data were compromised and to learn about the products the company was presumably providing to help them protect themselves from the effects of the hack.[89] But the website asked consumers for some of the very same information that Equifax had already left vulnerable to hackers, including the last six digits of consumers' social security numbers.[90] Then it misled consumers, telling *most* visitors the same thing: that their information *may* have been compromised, and instructing them to enroll in the Equifax credit monitoring program at some later date. [91]

And to make matters worse, according to cybersecurity experts consulted by Senator Warren's staff, EquifaxSecurity2017.com had major security vulnerabilities: the site Equifax took weeks to put up to handle inquiries and allow consumers to sign up for services that could protect their financial futures, was itself vulnerable. The main problem was that the site's design and web address made it easy for others to impersonate and collect consumers' information.[92] To demonstrate this, a cybersecurity expert created a website with a nearly identical web address – www.securityequifax2017.com – which looked so similar to the actual website's link that Equifax directed consumers to the fake site multiple times.[93]

In addition, experts consulted by Senator Warren's staff identified numerous other technical flaws in the website design. They reported that the website was set up to run on a stock installation of Wordpress, which didn't include the necessary security features to protect the sensitive information consumers submitted, and that the[94] website's Transport Layer Security certificate also did not perform proper revocation checks, which would have ensured that it was establishing a secure connection and protecting a user's data. And then, on October 12, Equifax was forced to take down a web-page where people could learn how to get a free credit report when a security analyst reported that the site's visitors were targeted by malicious pop-up ads.[95] After failing to protect consumer data, Equifax subsequently set up a website that put their customers in even greater danger.

4. Equifax Forced Arbitration Requirements

In the wake of the breach, Equifax urged all consumers to sign up for one year of free credit monitoring from TrustedID Premier, a product Equifax owned. But to sign up for this service, Equifax initially required consumers to sign a forced arbitration agreement and give up their right to go to court if Equifax cheated them in the future.[96] And deep in the fine print of the agreement was a provision that allowed Equifax to charge customers if they didn't cancel the service within a year.[97] Equifax ultimately eliminated both requirements by September 10, after a public outcry.[98]

5. Equifax Used the Breach as a Moneymaking Opportunity

Rather than acting solely to help customers after the breach, Equifax instead used it as a moneymaking opportunity, attempting to profit off of their own failures. Equifax initially charged consumers to freeze their credit.[99] A credit freeze prevents a credit reporting agency from providing a consumer's credit file to a third party that does not already have the consumers as a customer, and is often the best tool for consumers to protect themselves against identity theft. At first, Equifax was charging customers the full amount allowed – up to $30.95 per credit bureau – to freeze their credit in the wake of the breach.[100] Equifax was raking in these fees until the public backlash forced it to provide free freezes – but only until it releases a new "credit lock" product in 2018, which provides some of the same services without the legal protections.[101] Equifax controls its own credit lock product, which means it can control what services the product provides, whether customers are able to sue if Equifax provides data notwithstanding the lock, and whether it remains free after the public attention dissipates.

The problem for consumers is that risks will continue until well after Equifax's free service ends, and if they want to fully protect themselves, they may have little choice but to sign up for the new product. According to the FTC, "if certain types of information – such as Social Security numbers – are exposed due to a breach, the risks to consumers could certainly continue for longer than one year. …Given that Equifax has chosen to provide free credit monitoring for only one year, some consumers may choose to pay for credit monitoring services after that period."[102]

Equifax also made money on other companies' products after the breach. Frustrated customers who were fed up by Equifax's customer service or didn't trust Equifax's protection flocked to other companies like Lifelock, which reported a tenfold increase in enrollment during the month after the Equifax breach.[103] As Former Equifax CEO Rick Smith confirmed under questioning by Senator Warren, Lifelock uses Equifax to monitor its customers' credit and pays Equifax on a per customer basis for use of its services.[104]

Former Equifax CEO Richard Smith said in August – after Equifax had discovered the breach – that fraud "is a huge opportunity" for Equifax.[105] Equifax sells products to businesses and governments to help them prepare for and recover from data breaches.[106] They also sell credit monitoring products to help mitigate damages when breaches happen. As Senator Warren pointed out during a Banking Committee Hearing on October 4, 2017, "So far, 7.5 million people have signed up for free credit monitoring through Equifax since the breach. If just 1 million of them buy just one more year of monitoring through Equifax at the standard rate of $17 a month, that is more than $200 million in revenue for Equifax because of this breach."[107]

E. Federal Legislation is Necessary to Protect Consumers

Equifax and other credit reporting agencies collect consumer data without permission, and consumers have no way to prevent their data from being collected and held by the company.[108] Equifax recently confirmed to Senator Warren that the company "will not offer consumers the opportunity to delete their personally identifiable information…" [109] Equifax adopted weak cybersecurity measures that did not do enough to protect that data. This investigation conducted in the aftermath of the recent massive security breach reveals that the company failed to safeguard consumer data and was unable or unwilling to address persistent weaknesses in their system, even when notified by multiple parties, including the Department of Homeland Security. After hackers took advantage of one of these weaknesses to access the personal data of over 145 million consumers, Equifax caused consumers, investors, and the federal government even more problems by waiting 40 days to notify interested parties. And after finally announcing the breach, Equifax abandoned consumers once again by offering shoddy, unreliable assistance that failed to fix their problems and, in some cases, increased their risk.[110]

Individual companies have a responsibility to protect personal information. But federal legislation is necessary to give regulators and consumers the tools they need to ensure that credit reporting agencies, including Equifax, put consumer financial safety above their bottom-line. Legislation should:

- **Impose Appropriate Penalties in the Event of a Breach of Consumer Data**

The federal government cannot presently issue fines against credit reporting agencies when they fail to protect personal information and put consumer safety and financial security at risk – even when, like Equifax, they do so despite having ample warning of problems. In fact, the FTC has requested legislation that would "allow the FTC to seek civil penalties," because these penalties would "help ensure effective deterrence" of cybersecurity breaches." [111] The CFPB also supports such legislation, claiming that "federal laws that are applicable to data security have not kept pace with technological and cybersecurity developments… it is imperative for Congress to take steps to ensure that the regulatory framework is adequate to meet" the challenges posed by cybersecurity threats, and adding that "federal laws…have not kept pace with…cybersecurity developments."[112] There have been breaches at all three credit reporting agencies in the last several years, and hundreds of millions of consumers have been impacted.[113] When credit reporting agencies collect personal data without consumer permission, the burden should be on them to protect that data. If they fail to protect that data, they should be punished.

Consumer lawsuits do not provide adequate deterrence for companies like Equifax. While the average consumer recovers less than $2 through civil lawsuits in response to data breaches, Equifax is actually set to make money off their recent breach. If our laws don't punish companies like Equifax for their failure to protect sensitive consumer data, these companies will continue to adopt sub-standard security measures.

- **Set Strict Cybersecurity Standards and Empower the FTC to Update and Monitor these Standards**

No single agency currently has the appropriate authority to both establish basic cybersecurity requirements and monitor companies' adherence to those standards. The FTC itself has stated that "additional tools are necessary."[114] Equifax didn't just fall victim to a sophisticated attacker; Equifax failed to provide basic security for the personal information belonging to millions of Americans. Congress should empower the FTC to establish requirements

for fundamental cybersecurity measures at credit reporting agencies.

The FTC should also have supervisory authority to monitor credit reporting agencies and ensure they are following these standards. If they aren't, the FTC should be able to obtain an injunction requiring them to update their security procedures. If a company like Equifax has a breach and the FTC finds that they weren't following the appropriate standards, the penalties should be increased for every consumer exposed in the breach. That is the only way to make sure credit reporting agencies take the security of consumer data seriously.

Equifax and other credit reporting agencies have taken advantage of consumers for years, collecting their data without permission and turning a huge profit while failing to adequately protect that data. These practices won't change without federal legislation that forces Equifax and its peers to put appropriate emphasis on protecting consumer data.

Endnotes

1 Equifax, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sep. 7, 2017) (https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628).

2 AnnaMaria Andriotis and Robert McMillan, "Equifax Security Showed Signs of Trouble Months Before Hack," Wall Street Journal (Sept. 26, 2017) (https://www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947).

3 Prepared Testimony of Richard F. Smith before the U.S. Senate Committee on Banking, Housing, and Urban Affairs (Oct. 4, 2017) (http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf).

4 Id.

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

6 Senator 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); Senator Elizabeth Warren, Warren Presses Former Equifax CEO Richard Smith for More Answers on Data Breach (Oct. 12, 2017) (https://www.warren.senate.gov/?p=press_release&id=1954); Senator Elizabeth Warren, Senator Warren Asks Former Equifax CEO if Breach Created New Business Opportunities for the Company (Oct. 4, 2017) (https://www.warren.senate.gov/?p=press_release&id=1931).

7 "Former Equifax CEO Faces Congress," Wall Street Journal (Oct. 4, 2017) (https://www.wsj.com/livecoverage/equifax-hack-hearing-1003/card/1507123932); "2016 Annual Report," Equifax (https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf); "2015 Annual Report," Equifax (https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2015-annual-report.pdf).

8 "2016 Annual Report," Equifax (https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf); "2015 Annual Report," Equifax (https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2015-annual-report.pdf).

9 See AnnaMaria Andriotis and Robert McMillan, "Equifax Security Showed Signs of Trouble Months Before Hack," Wall Street Journal (Sept. 26, 2017) (https://www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947?mod=e2tw); Consultation with Independent Experts.

10 *Supra* note 5.

11 "Equifax Response to Senator Warren and Executive Summary," Mandiant and Equifax (received Oct. 1, 2017).

12 Equifax Briefing for Senate Banking Committee Staff, Dec. 11, 2017.

13 *Id.*

14 *Id.*

15 *Supra* note 11.

16 Id.; *Supra* note 5.

17 *Supra* note 11; Consultation with Independent Experts.

18 *Id.*

19 *Id.*

20 *Id.*

21 See *Id.*

22 *Id.*

23 "Rick Smith, CEO, Equifax," YouTube (Aug. 22, 2017) (https://www.youtube.com/watch?v=lZzqUnQg-Us).

24 *Supra* note 12.

25 *Supra* note 23.

26 "Prepared Testimony of Richard F. Smith before the U.S. Senate Committee on Banking, Housing, and Urban Affairs," U.S. Senate (Oct. 4, 2017) (https://www.banking.senate.gov/public/_cache/files/da2d3277-d6f4-493a-ad88-c809781f7011/F143CC8431E6CD31C86ADB64041FB31B.smith-testimony-10-4-17.pdf).

27 *Id.*

28 *Id.*

29 *Id.*

30 "Forensic Investigation and Remediation," Briefing from Russ Ayres, Chief Security Officer of Equifax (Dec. 11, 2017).

31 *Supra* note 1.

32 *Id.*

33 *Id.*

34 *Id.*

35 *Id.*

36 "Prepared Testimony of Richard F. Smith before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection," U.S. House of Representatives (Oct. 3, 2017) (http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf).

37 *Supra* note 12.

38 Answer to Question 27, Equifax's Response to Banking Committee Questions for the Record (provided on January 2, 2017).

39 *Supra* note 35.

40 *Supra* note 12.

41 See Answer to Question 103, Equifax's Response to Banking Committee Questions for the Record (provided on January 2, 2017)

42 "Consumer Notice," Equifax Security 2017 (https://www.equifaxsecurity2017.com/consumer-notice/).

43 "CF Disclosure Guidance: Topic No. 2," SEC Division of Corporation Finance (Oct. 13, 2011). (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm).

44 *Id.*

45 "Equifax INC Company Filings," SEC EDGAR (last accessed Nov. 1, 2017) (https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&CIK=0000033185&owner=include&count=40&hidefilings=0); "Form 8-K," SEC EDGAR (Sept. 7, 2017) (https://www.sec.gov/Archives/edgar/data/33185/000003318517000026/a8-kcover20170907.htm).

46 "Investor Relations," Equifax (Aug. 2017) (https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/presentation/investor-relations-presentation-august-2017.pdf).

47 Letter from Acting Chairman Maureen Ohlhausen to Senator Elizabeth Warren, October 3, 2017.

48 "Bureaus & Offices," Federal Trade Commission (https://www.ftc.gov/about-ftc/bureaus-offices).

49 Letter from King and Spalding, LLP to Senator Elizabeth Warren, October 1, 2017.

50 Letter from Acting Chairman Maureen Ohlhausen to Senator Elizabeth Warren, October 3, 2017.

51 Letter from King and Spalding, LLP, Counsel for Equifax to Senator Elizabeth Warren, October 1, 2017.

52 October 18, 2017 IRS Briefing for Senator Warren's staff.

53 "Search Results" USA Spending (number current as of Dec. 4, 2017) (https://www.usaspending.gov/Pages/AdvancedSearch.aspx?k=Equifax).

54 *Id.*

55 Evan Sweeney, "ACA data unscathed in Equifax breach as lawmakers contemplate mnore rigorous cybersecurity regulations," Fierce Healthcare (Sept. 12, 2017) (https://www.fiercehealthcare.com/privacy-security/aca-data-unscathed-equifax-data-breach-as-lawmakers-contemplate-more-rigorous).

56 USA Spending, Equifax Results Summary Record GS22F9663D (https://www.usaspending.gov/Pages/AdvancedSearch.aspx?sub=y&ST=C,G,L,O&FY=2016,2015&A=0&SS=USA&AA=2000&AB=2050&k=Equifax).

57 Steven Overly and Nancy Scola, "IRS awards multimillion-dollar fraud-prevention contract to Equifax," Politico (Oct. 3, 2017) (https://www.politico.com/story/2017/10/03/equifax-irs-fraud-protection-contract-243419).

58 Id.; "Letter from Senators Elizabeth Warren and Ben Sasse to Acting IRS Commissioner John Koskinen," (Oct. 5, 2017) (https://www.warren.senate.gov/?p=press_release&id=1934).

59 Julia Horowitz, "IRS suspends its contract with Equifax amid new security concerns," CNN (Oct. 13, 2017) (http://money.cnn.com/2017/10/13/news/equifax-irs-contract-suspended/index.html).

60 October 18, 2017 IRS Briefing for Senator Warren's staff.

61 *Id.*

62 *Id.*

63 "Decision: Equifax Information Services, LLC," Government Accountability Office (Oct. 16, 2017) (https://www.gao.gov/assets/690/687765.pdf).

64 *Id.*

65 *Id.*

66 Under federal law, the IRS could not begin this process unless it found that "compelling circumstances that significantly affect interests of the United States will not permit waiting for the decision," 31 USC §3553, a standard that courts have interpreted to be a high threshold and IRS lawyers believed was not met. October 18, 2017 IRS Briefing for Senator Warren's staff.

67 October 18, 2017 IRS Briefing for Senator Warren's staff.

68 Id.; Frank Konkel, "GAO Denies Equifax Bid Protect on IRS Contract," Nextgov (Oct. 16, 2017) (http://www.nextgov.com/cio-briefing/2017/10/gao-denies-equifax-bid-protest-irs-contract/141807/).

69 "Letter from Senators Elizabeth Warren and Ben Sasse to Acting IRS Commissioner John Koskinen," (Oct. 5, 2017) (https://www.warren.senate.gov/?p=press_release&id=1934).

70 October 18, 2017 IRS Briefing for Senator Warren's staff.

71 *Id.*

72 *Id.*

73 Meredith Somers, "IRS suspends Equifax contract as 'precautionary step' following credit agency's data breach," Federal News Radio (Oct. 13, 2017) (https://federalnewsradio.com/management/2017/10/irs-suspends-equifax-contract-as-precautionary-step-following-credit-agencys-data-breach/).

74 October 18, 2017 IRS Briefing for Senator Warren's staff.

75 "Equifax Announces Cybersecurity Incident Involving Consumers Information," Equifax (Sept. 7, 2017) (https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628).

76 See Equifax Crisis Management Plan, Version 5.0 (May 2017) (provided in response to Banking Committee Questions for the Record).

77 Consumer Financial Protection Bureau's Response to Senator Warren's Letter, Nov. 21, 2017.

78 *Id.*

79 *Supra* note 11.

80 Equifax Crisis Management Plan, Version 5.0 (May 2017) (provided in response to Banking Committee Questions for the Record).

81 Equifax, Security Incident Handling Policy and Procedures (October 2014) (provided in response to Banking Committee Questions for the Record)

82 Equifax Crisis Management Plan, Version 5.0 (May 2017) (Bates # EFXCONG-SBC000000022) (provided in response to Banking Committee Questions for the Record).

83 Equifax, Security Incident Handling Policy and Procedures (October 2014) (Bates # EFXCONG-SBC000000156) (provided in response to Banking Committee Questions for the Record).

84 Equifax, Security Incident Handling Policy and Procedures (October 2014) (Bates # EFXCONG-SBC000000156) (provided in response to Banking Committee Questions for the Record).

85 Brian Fung, "I called Equifax with a simple question. This is what happened." Washington Post (Sept. 13, 2017) (https://www.washingtonpost.com/news/the-switch/wp/2017/09/13/i-called-equifax-with-a-simple-question-this-is-what-happened/).

86 Id.

87 Id.

88 *Supra* note 73.

89 *Supra* note 1.

90 Hamza Shaban and Hayley Tsukayama, "Equifax asks consumers for personal info, even after massive data breach," Washington Post (Sept. 8, 2017) (https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/after-data-breach-equifax-asks-consumers-for-social-security-numbers-to-see-if-theyve-been-affected/).

91 Sarah Buhr, "PSA: no matter what, Equifax may tell you you've been impacted by the hack," Tech Crunch (Sept. 8, 2017) (https://techcrunch.com/2017/09/08/psa-no-matter-what-you-write-equifax-may-tell-you-youve-been-impacted-by-the-hack/); Ron Lieber, "Equifax's Instructions Are Confusing. Here's What to Do Now." New York Times (Sept. 8, 2017) (https://www.nytimes.com/2017/09/08/your-money/identity-theft/equifaxs-instructions-are-confusing-heres-what-to-do-now.html).

92 Merrit Kennedy, "After Massive Data Breach, Equifax Directed Customers To Fake Site," NPR (Sept. 21, 2017) (http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed-customers-to-fake-site).

93 *Id.*

94 Dan Goodin, "Why the Equifax breach is very possibly the worst leak of personal info ever," Ars Technica (Sept. 8, 2017) (https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/).

95 Selena Larson, "Equifax is dealing with yet another security issue," CNN (Oct. 12, 2017) (http://money.cnn.com/2017/10/12/technology/equifax-website-adware/index.html?iid=EL).

96 David Lazarus, "The real outrade isn't Equifax's arbitration clause – it's all the others," LA Times (Sept. 12, 2017) (http://www.latimes.com/business/lazarus/la-fi-lazarus-equifax-arbitration-clauses-20170912-story.html).

97 Carla Herreria, "Equifax Clarifies Policy After Outcry Over Consumers' Legal Rights Following Hack," Huffington Post (Sept. 9, 2017) (https://www.huffingtonpost.com/entry/equifax-changes-arbitration-clause-victims-of-security-breach_us_59b364fae4b0dfaafcf81bf7).

98 Brian Fung, "Equifax finally responds to swirling concerns over consumers' legal rights," Washington Post (Sept. 10, 2017) (https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/); Ken Sweet, "New Lawsuits, Gestures to Customers in Equifax Data Breach," U.S. News (Sept. 12, 2017) (https://www.usnews.com/news/business/articles/2017-09-12/new-lawsuits-gestures-to-customers-in-equifax-data-breach).

99 Ron Lieber, "Equifax, Bowing to Public Pressure, Drops Credit-Freeze Fees," New York Times (Sept. 12, 2017) (https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html).

100 Sarah O'Brien, "Here's what it costs to freeze your credit after Equifax breach," CNBC (Sept. 15, 2017) (https://www.cnbc.com/2017/09/15/heres-what-it-costs-to-freeze-your-credit-after-equifax-breach.html); Mariella Moon, "Equifax waives credit freeze fees after facing backlash," Engadget (Sept. 13, 2017) (https://www.engadget.com/2017/09/13/equifax-waives-credit-freeze-fees/).

101 Octavio Blanco, "Why a Credit Freeze Is Better Than a Credit Lock," Consumer Reports (Sept. 28, 2017) (https://www.consumerreports.org/credit-bureaus/why-credit-freeze-is-better-than-credit-lock/); Jackie Wattles, "Equifax to offer free program to lock and unlock credit files for life," CNN Money (Sept. 27, 2017) (http://money.cnn.com/2017/09/27/news/companies/equifax-credit-freeze-free/index.html).

102 Letter from Maureek K. Ohlhausen, Acting FCC Chairman, to Senator Warren (Oct 4, 2017).

103 Hearing Transcript, October 4, 2017 pg 44 ln 1; Polly Mosendz, "After the Equifax Hack, LifeLock Sign-ups Jump Tenfold," Bloomberg (Sept. 13, 2017) (https://www.bloomberg.com/news/articles/2017-09-13/after-the-equifax-hack-lifelock-sign-ups-jump-tenfold).

104 *Id.*

105 *Supra* note 23.

106 "Equifax Breach Products," Equifax (http://www.equifax.com/business/equifax-breach-products/).

107 Hearing Transcript, October 4, 2017 pg 43 ln17–24.

108 Answer to Question 162, Equifax's Response to Banking Committee Questions for the Record (provided on January 2, 2017).

109 Answer to Question 162, Equifax's Response to Banking Committee Questions for the Record (provided on January 2, 2017).

110 Selena Larson, "Equifax is dealing with yet another security issue," CNN (Oct. 12, 2017) (http://money.cnn.com/2017/10/12/technology/equifax-website-adware/index.html).

111 "FTC Letter to Senator Warren," Federal Trade Commission (Oct. 4, 2017).

112 *Supra* note 73.

113 Robert Westervelt, "Equifax, Other Credit Bureaus Acknowledge Data Breach," CRN (Mar. 13, 2013) (http://www.crn.com/news/security/240150683/equifax-other-credit-bureaus-acknowledge-data-breach.htm); "Experian Breach Affects 15 Million Consumers," Krebs on Security (Oct. 2, 2015) (https://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/); Thomas Fox-Brewster, "A Brief History of Equifax Security Fails," Forbes (Sept. 8, 2017) (https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#15441c08677c).

114 "FTC Letter to Senator Warren," Federal Trade Commission (Oct. 4, 2017).