HARVARD | BUSINESS | SCHOOL

9-118-031

REV: APRIL 25, 2019

SURAJ SRINIVASAN

QUINN PITCHER

JONAH S. GOLDBERG

Data Breach at Equifax

It was October 4, 2017, and Richard Smith, the former CEO of Equifax, had just finished testifying before the U.S. Senate Committee on Banking, Housing, and Urban Affairs. He had been called before the Committee to address the data breach Equifax had experienced between May and July earlier that year, which exposed personal information about over 145 million Americans. Smith had resigned just over a week earlier, the latest casualty of the massive crisis at the credit reporting agency, which had claimed the jobs of two other executives and spawned insider trading allegations, investigations, and dozens of lawsuits.[a]

Observers were critical of Equifax's cybersecurity preparedness, as reports surfaced that the company had been notified about the software vulnerability exploited by its attacker in early March but had failed to fix it on time. They were also critical of the company's response to the breach, especially the delay between when Equifax discovered the breach (July 29) and when it disclosed it to the public (September 7). Others questioned why the board was not notified until three weeks after the breach was uncovered and whether the board's response was adequate.

Smith's replacement, interim CEO Paulino do Rego Barros, Jr., and the board needed to respond to these criticisms. Facing an onslaught of lawsuits and investigations, Equifax had to improve its cybersecurity systems and convince both consumers and public officials that it remained a reliable steward of sensitive information. Accomplishing this, however, appeared easier said than done.

Equifax

Founded in 1899, Equifax Inc. (Equifax) was a U.S. credit reporting company. Along with Experian and TransUnion, Equifax was one of the three main credit reporting companies, responsible for collecting and providing information on income and credit-worthiness to organizations and

[a] The multiple congressional investigations into the breach (by the Senate Committee on Banking, Housing, and Urban Affairs, the Senate Committee on Homeland Security and Government Affairs, and the House of Representatives Committee on Oversight and Government Reform) produced a number of reports detailing the causes and consequences of the exfiltration of consumer data. These reports will be referenced throughout the case as the products of Congressional investigations.

Professor Suraj Srinivasan and Research Associates Quinn Pitcher and Jonah S. Goldberg prepared this case. This case was developed from published sources. Funding for the development of this case was provided by Harvard Business School and not by the company. HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.

individuals. "Powering the world with knowledge," the company's slogan, captured its aspirations. The company wrote in its 2016 annual report that:

> We leverage some of the largest sources of consumer and commercial data, along with advanced analytics and proprietary technology, to create customized insights which enable our business customers to grow faster, more efficiently and more profitably, and to inform and empower consumers. Businesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning[b] technology, marketing tools, debt management and human resources-related services. We also offer a portfolio of products that enable individual consumers to manage their financial affairs and protect their identity.

Equifax collected consumer and business credit information from banks, analyzed it using proprietary processes, and sold the credit analysis, generating a gross margin of around 90 percent. Equifax managed data on more than 820 million consumers and over 91 million businesses around the world.[1]

Equifax's primary business was its U.S. Information Services (USIS) segment, which comprised online information services, mortgage solutions, and financial marketing services. The first two services derived revenue from the sale of consumer and commercial credit reports and scores. Credit reports contained personal information including bill payment history, loans, debt, residency, and work history, providing a thorough picture of an individual or organization's credit-worthiness. Lenders used credit reports to assess loan and credit applications.[2]

In Equifax's Workforce Solutions segment, the same data collected for consumer credit reports was sold to organizations looking to verify individual employment and income history. Equifax also offered businesses services for handling unemployment claims, employment-based tax credits, and other similar programs. The company further operated a Global Consumer Solutions segment that provided credit monitoring and identity theft protection products in the U.S., Canada, and U.K.[3]

Equifax had seen great success, driven by its data collection and analysis services. During Smith's tenure as CEO (from September 2005 to September 2017), its stock price had more than quadrupled, and the company had engaged in fifteen acquisitions.[4]

Cybersecurity at Equifax

The Reporting Structure

Its information-intensive business model made the company attractive to cybercriminals. Information security was therefore paramount for the company. Equifax wrote in its 2016 annual report:

> We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact.[5]

After Smith was appointed CEO in 2005, the company invested millions in cybersecurity measures. This effort continued over time, with Equifax spending around one percent of its operating revenue on cybersecurity each year between 2014 and 2017.[6] Early in his tenure, Smith brought on a cybersecurity

[b] In its 2016 annual report, Equifax described this as "decisioning software services, which facilitate and automate a variety of consumer and commercial credit-oriented decisions." 2016 Annual Report. Equifax, Inc., p. 12.

expert, Tony Spinelli, as chief security officer (CSO), and Spinelli worked to modernize Equifax's cyber defenses, rehearsing possible breaches and creating "24-hour crisis-management squads" that would remediate issues as they arose. Spinelli and his top deputy left Equifax in 2013, followed by a number of other senior cybersecurity employees."[7]

Information security responsibilities at Equifax had been divided between two different chains of command. The first of these was legal/security chain of command. Here, the chief legal officer (CLO) supervised the CSO, who managed the security group, which comprised between 180 and 190 employees at the time of the breach. At the time of the breach, the CLO John Kelley, lacked a background in IT or security and had been in the position since 2013. The CSO was Susan Mauldin, a former software engineer who had transitioned into managing corporate information security systems some years prior to joining Equifax. The second chain of command dealt with information technology (IT). It was headed by the chief information officer (CIO), David Webb. Webb had joined Equifax in 2010 after three decades of working in IT.[c] Webb and Kelley reported directly to the CEO, Richard Smith.[8]

Webb described the division of responsibilities between the security and the IT organizations as follows:

> Typically, the way the work was separated between the organizations, the Security organization would define the 'what.' They had a security engineering function. The IT guys were responsible for deploying the technology that [Security] wanted into the infrastructure, and then [Security] would be provided the ability to configure the software, all the solution [sic], the appliance, whatever it might be, in accordance with their desires.[9]

He continued:

> The policy was typically defined within the Security organization. . . . The IT organization would be responsible for ensuring that, in the case, for example, of a patch, that the patch was applied. Because the Security organization could not effect changes to the infrastructure directly. They could operate software, but they could not install the software and they could not change the infrastructure."[10]

In addition to these executives, Graeme Payne, the Senior Vice President and CIO for Global Corporate Platforms (from July 2014 to October 2017, previously Equifax's Vice President of IT Risk and Compliance from March 2011), supervised important cybersecurity functions at Equifax. Payne reported to Webb, the CIO, and was responsible for overseeing "access management, IT-audit coordination, and IT-Security coordination" at the time of the breach.[11]

A number of teams dealt with cybersecurity issues at Equifax. Among them were the Global Threat and Vulnerability Management (GTVM) team, the Vulnerability Assessment team, and the Countermeasures team. The GTVM team tracked threats to the security of Equifax's IT systems and notified relevant personnel across the company about such threats through emails and monthly meetings. The Vulnerability Assessment team ran regular scans of Equifax's IT systems for vulnerabilities, and the Countermeasures team deployed code designed to obstruct the exploitation of ongoing vulnerabilities while IT "system owners" installed patches to resolve the underlying software problems.[12]

[c] Mauldin and Webb both resigned in September 2017, following the fallout from the breach.

Prior Security Issues

Prior to the breach in 2017, Equifax had suffered several security lapses. Between April 2013 and January 2014, hackers accessed credit report data from Equifax. In 2015, a "technical error" ostensibly caused by software modifications publicly exposed consumer information. In 2016, another incident exposed the salary and tax data of 431,000 employees at Equifax client Kroger. Finally, in February 2017, Equifax discovered that hackers were exploiting Equifax Workforce Solutions, downloading employee tax documents on Equifax clients like Northrop Grumman and Whole Foods. Equifax retained cybersecurity firm Mandiant to investigate the Workforce Solutions incident in March. While conducting its investigation, Mandiant "warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems."[13]

Equifax had received other warnings about potential cybersecurity vulnerabilities. In December 2016, an independent researcher discovered that Equifax had left consumer information exposed on a website accessible to any internet user (apparently intended for employees only). The researcher alerted Equifax to the vulnerability, but the company did not take down the website until June 2017. Equifax had also hired professional services firm Deloitte to perform a security audit in 2016. The audit identified several issues, including, said a former employee, "a careless approach to patching systems." Another former employee said that attempts to address the audit went unheeded, "Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking."[14]

Several cyber risk analysis firms had previously found that Equifax was ill-prepared to prevent and respond to a data breach. In April 2017, Cyence, a cybersecurity firm specializing in quantifying the financial impact of cyber risks, assessed a 50 percent probability that Equifax would experience a breach in the coming year and found the company's cybersecurity measures second-to-last in a peer group of 23 financial services firms. Other reports identified issues with Equifax's data hygiene. Fair Isaac Corp. (FICO), which analyzed corporate cyber risk for insurance underwriting purposes, assigned Equifax an enterprise security score of around 550 on a scale of 300 to 850 and found that public websites run by Equifax "had expired certificates, errors in the chain of certificates or other web-security issues" as recently as July 2017. On a scale of A-F, with F being the worst, BitSight Technologies—a cybersecurity research firm—gave Equifax an F grade for application security and a D for software patching.[15]

MSCI's ESG research team was especially critical of Equifax's cybersecurity preparedness, giving the company a rating of zero for privacy and data security in April 2017 and an overall ESG rating of CCC (its lowest possible rating, given to just five percent of companies).[d] Specifically, MSCI noted, "The company's data and privacy policies are limited in scope and Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems." Because all of Equifax's revenue relied on the use of personal data, MSCI believed this exposed the company to serious regulatory risk.[16]

The Apache Struts Vulnerability

In early March 2017, a cybersecurity researcher discovered a security flaw in Apache Struts, an open source software used to build web applications in Java by organizations ranging from banks to government agencies. The researcher provided his findings to the Apache Foundation, the non-profit responsible for maintaining and updating the software, which published the research findings and a software patch for the issue on March 6.[17] Researchers at Cisco Systems sent out a warning about the vulnerability on March 8.[18]

[d] MSCI scored other companies in Equifax's peer group as high as a 9.5 out of 10 on privacy and data security.

The vulnerability was especially dangerous because it was accessible through two publicly available exploits. Hackers could simply scan for servers running Apache Struts that had yet to be patched, and upon identifying such servers, try to exploit the weakness. Once an exploit was executed, the hacker could add their own code to webpages, disable firewalls, and install malware with their IP address masked to prevent tracing.[19] This process was not especially difficult either. A Senate investigation found that "individuals with basic computer skills – not just skilled hackers – could follow published instructions and exploit the vulnerability."[20]

The popularity of the software and the seriousness of the vulnerability led the U.S. Department of Homeland Security's Computer Emergency Readiness Team (CERT) to alert potentially vulnerable parties, also on March 8.[21] Among those notified were Equifax's GTVM team and Mauldin, its CSO. Equifax used Apache Struts as the middleware for its Automated Consumer Interview System (ACIS), a web portal that allowed consumers to dispute items in their credit reports.[22]

On March 9, the GTVM team circulated CERT's notification to approximately 430 Equifax employees on relevant listservs. Under Equifax's internal policies, the Apache Struts patch was "critical" and therefore needed to be implemented within 48 hours of its release.[23] Nonetheless, in Smith's words, "The vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification."[24]

While the vulnerability was discussed in some depth at the GTVM team's monthly threat meeting, on March 16, 2017, the majority of senior Equifax managers with cybersecurity responsibilities did not generally attend these meetings. No one was required to attend them, and the company neglected to log which employees chose to attend. Many employees did receive the slide deck presented at the meeting via email, which included the Apache Struts patch on a list of necessary software patches, as well as a list of the compromised versions of Apache Struts and specific instructions explaining how to update them. Because old vulnerabilities typically were not included in subsequent months' GTVM slide decks, the Apache Struts vulnerability was absent from the list of necessary patches in the April 2017 deck.[25]

As a stopgap measure prior to patching a vulnerability, those responsible for the security of a vulnerable system often installed signatures and rules to identify and obstruct efforts to exploit the vulnerability in question. At Equifax, the installation of such signatures and rules was handled by the Countermeasures team. By the day that the GTVM team received CERT's alert about the vulnerability, two different threat intelligence providers had already released signatures designed to defend against related attacks, but because of technical issues, it took the Countermeasures team until March 14 to install them. The day that these signatures were installed on Equifax systems, they blocked a "significant number" of attempts to infiltrate the company's network via the Apache Struts vulnerability. Subsequently, both Equifax's Vulnerability Assessment team and its GTVM team ran scans of the company's systems for vulnerable versions of Apache Struts, and neither team's scans yielded any results.[26]

The Breach

Hackers scanning for the unpatched vulnerability discovered it on an Equifax server on March 10. From there, an "entry crew" breached Equifax using the Apache Struts vulnerability before handing the operation off to a more sophisticated team, which worked over the next several months to establish access to dozens of Equifax databases (see **Exhibit 1** for a technical explanation of the hack). The new team created over 30 backdoors into Equifax's systems using web shells registered to unique internet addresses (increasing the difficulty of finding them all).[27] From May 13 onward, the hackers began collecting personal identifying information (PII).

The hackers continued to amass PII from Equifax's servers until mid-summer. On the evening of July 29, Equifax's Countermeasures team updated 74 Secure Sockets Layer (SSL) certificates on a variety of different applications, including the ACIS portal. SSL certificates were a key component of a security protocol that allowed for encrypted data exchange between web browsers and servers. Typically, the certificates needed to be renewed between every 12 and 39 months in order to stay active, and over previous years, Equifax had allowed hundreds to expire across its network. Updating the ACIS certificate reactivated an "SSL visibility appliance," which allowed the Countermeasures team to monitor traffic on the ACIS portal. When the SSL visibility appliance was reactivated, it showed ACIS traffic from an IP address in China. This jumped out to the Countermeasures team because Equifax did not operate in China. They promptly blocked the IP address. The next day, they noticed additional ACIS traffic from another IP address associated with a Chinese entity and decided to take the ACIS portal offline, preventing further access by the hackers.[28]

When Equifax discovered the extent to which it had been breached, it completely shut down its dispute portal for 11 days while its cybersecurity staff worked to identify every entry point. Webb, the CIO, informed Smith of the suspect activity on July 31, but Webb did not make clear that PII had been stolen at that time. On August 2, Equifax hired the law firm King & Spalding LLP as well as Mandiant to investigate the breach and reported the suspicious activity on its network to the U.S. Federal Bureau of Investigation (FBI).[29]

On August 11, Equifax and Mandiant's investigation discovered that hackers had been able to go beyond the data contained in the dispute portal and "may have accessed a database table containing a large amount of consumer PII, and potentially other data tables." Smith was informed that consumer PII had been stolen on August 15. At an investor presentation the next day, Smith did not mention anything about the ongoing investigation or potential breach. On August 17, Smith held a senior leadership meeting to receive a "detailed briefing" on the investigation, and on August 22, he first notified a member of the board, lead director Mark Feidler, about the breach. The full board was informed via telephone meetings on August 24 and 25. Smith said, "on September 1, I convened a Board meeting where we discussed the scale of the breach and what we learned so far, noting that the company was continuing to investigate." Equifax's investigation team finalized its initial list of the 143 million people then believed to have been affected on September 4.[30]

The hackers obtained names, Social Security numbers, birth dates, and addresses for each of those 143 million people, and for a smaller number, email addresses, driver's license numbers, credit card numbers, passport numbers, tax identification information, and credit report dispute documents.[31]

Sources of Vulnerability Inside Equifax

Internal Controls and the Patch Management Process

During his congressional testimony, Smith faulted a single employee for the failure to implement the software patch, suggesting that the vulnerability hadn't been addressed because a manager had neglected to forward a warning email.[32] In an interview with congressional investigators, Graeme Payne expressed his belief that Smith had been referring to him; Payne then disputed Smith's characterization, saying:

> To assert that a senior vice president in the organization should be forwarding vulnerability alert information to people . . . sort of three or four layers down in the organization on every alert just doesn't hold water, doesn't make any sense. If that's the process that the company has to rely on, then that's a problem.[33]

Payne did not believe it was his job to pass the GTVM email on to anyone. He claimed that he was never instructed to forward emails of this type, and he believed that he had received the email "for informational purposes."[34] Payne noted that the responsibility for resolving software vulnerabilities at Equifax was determined by the company's patch management policy. The patch management policy designated three different roles in implementing software patches. The "business owner" was charged with determining when the implicated systems were to be taken offline so that they could be patched. The "system owner" was then charged with patching the software in question, and the "application owner" was charged with making sure that the software had been fixed. Congressional reports differed on whether the occupants of these roles were formally designated at all, but at a minimum, such designations were "ambiguous." For his part, Payne was quite sure he was not one of them, and he did not believe it was his responsibility to notify the system owners and application owners under his supervision of the vulnerability because the patch management policy required all of them to subscribe to "vulnerability distribution bulletins," including the bulletin published by CERT.[35]

As the company's CIO and CSO testified to Congress, "[T]here were no redundancies within the patching process to ensure the proper individuals were notified of the need to patch." An internal audit Equifax conducted of its patch management infrastructure in 2015, concluded that the whole process took place on "the honor system."[36]

That 2015 internal audit identified a number of significant problems with Equifax's patch management process (resulting in a backlog of 8,500 unpatched vulnerabilities), and in 2017, many of those problems remained unresolved. In fact, when in August of 2017, Equifax was investigating security flaws in its ACIS system, three of the six flaws it identified had also been raised in the 2015 patch management audit.[37] One of these three of particular importance was Equifax's lack of a comprehensive inventory of its IT assets. Although the company had a number of different inventories, they were dispersed across different divisions within the organization, and none of them were comprehensive. This left both Equifax's security personnel and Payne himself, who was in charge of IT for ACIS system, unaware that ACIS ran Apache Struts until July 2017.[38]

Another flaw identified in the 2015 audit that had not been fully addressed by 2017 was that Equifax's approach to patching was reactive rather than proactive. This meant that rather than installing every software patch released for programs it used, Equifax only installed those software patches that were shown to be necessary to address specific vulnerabilities. Per the 2015 audit, this created a lag in the installation of critical patches – they were only installed after it had already become clear that failing to install them jeopardized the security of company systems, leaving those systems exposed in the interim. Moreover, the audit found that Equifax had no system in place to verify that identified vulnerabilities had, in fact, been successfully patched. Though the company ran regular scans to identify vulnerabilities, those scans were imperfect, and they were generally not subjected to scrutiny. Accordingly, if a vulnerability stopped turning up in scan results, Equifax assumed it had been adequately addressed, even though in some cases, it had not. In addition, Equifax's patch management process failed to prioritize patching "critical" technology assets over patching less important technology assets, allowing longer-than-necessary lag times for the implementation of essential patches. Senate investigators found that all of these flaws persisted through the time of the breach.[39]

Equifax employees identified three reasons for weaknesses in patch management. First, because Equifax, as a company, had grown for many years by acquiring other companies, its technology systems were not well-integrated with one another, rendering certain system-wide security scans and updates difficult. Second, many of Equifax's key technology assets ran on antiquated systems that would need to be updated themselves in order for the company to meet its own goals with respect to information security, but updating these fundamental systems "would lead to significant operational

risk." Third, Equifax simply did not have the personnel necessary to implement the technologies and processes that would be required to meet those internal security goals (see **Exhibit 2** for a comparison of Equifax's cybersecurity procedures with its competitors').[40]

The "Accountability Gap" in the Organizational Structure

A Congressional investigation found that part of the reason why Equifax lacked a consolidated inventory of IT assets was related to how it organized its IT and security personnel. Until 2005, Equifax's CSO reported to its CIO, who reported to the CEO, as is the practice at between one-quarter and one-half of companies with such positions. This structure integrated IT and security under one unified chain of command and was understood, even by Equifax's CIO at the time of the breach, to be an industry best practice. If the CSO did not report to the CIO, the other common structure at large companies was for the CIO and the CSO to be positions of equal status that both reported directly to the CEO and the board of directors. In 2005, however, spurred by an interpersonal conflict between its CIO and CSO (both of whom had left the company by 2013), Equifax moved its information security unit out from under the CIO's supervision and instead placed it under the supervision of the company's CLO, making the CLO the "head of security," a structure only employed at around eight percent of companies with such positions.[41]

In the view of the investigation, this division between the security and the IT organizations created an "accountability gap" in Equifax's information security infrastructure.[42] The House Committee's report identified the problem as follows:

> Depending on the organizational reporting structure a company adopts the CSO and CIO roles can be conflicting or complementary. At Equifax, the IT and Security organizations were siloed, meaning information rarely flowed from one group to the other. Collaboration between IT and Security mostly occurred when required, such as when Security needed IT to authorize a change on the network. Communication and coordination between these groups was often inconsistent and ineffective at Equifax.[43]

In April 2016, an internal restructuring of the IT organization led to the establishment of monthly meetings between the IT and Security leadership. These meetings aimed to ameliorate the problems of communication and coordination that had plagued the two divisions' relationship. They were attended by Webb, Payne, Mauldin, and Kelley, among others. Though Payne testified that key vulnerabilities implicated in the data breach (like problems with patch management and digital certificate deployment) were discussed during the meetings, they were not resolved in time to fend off the Apache Struts hacks.[44]

Similarly, Smith's quarterly senior leadership meetings also failed to compensate for the absence of "clear lines of accountability for developing IT security policies and executing these policies." Because Mauldin, the CSO, was not considered a member of the senior leadership, she was not generally in attendance. This meant that Smith did not receive regular updates about the status of security concerns at Equifax. To the extent that security concerns were represented in these meetings, they were represented by the CLO, who, as mentioned earlier, had no experience or training in information security.[45]

Technological Barriers to Effective Oversight

According to a Congressional report, the final major obstacle to effective information security oversight at Equifax was that its dated technology made it difficult for the company's IT and security teams to identify and address potentially malicious activity on its servers. The ACIS system through which the Apache Struts hackers gained access to Equifax's network, for example, dated back to the 1970s, when it had been custom-built for the company to comply with the Fair Credit Reporting Act.

The report further found that because of its age and proprietary nature, the ACIS system was "extremely difficult to patch, monitor, or upgrade." In fact, the only people who were capable of maintaining the system were a handful of its original developers, who fortunately still worked for Equifax in 2017, but there were not many of them left.[46]

Congressional investigators concluded that, in part because of these difficulties, Equifax's technological infrastructure lacked three fairly standard security features which, had they been in place, would have made the breach far easier to detect and remediate. First, the ACIS system in particular lacked file integrity monitoring (FIM) processes. FIM processes scanned for unauthorized or otherwise suspicious alterations in IT systems, configurations, or application software files, allowing for the quick detection of the vast majority of common cyberattack strategies. Experts believed that if Equifax had had FIM processes in place in 2017, it would have detected the breach before a significant amount of data was stolen. Mauldin, the CSO, was unaware that the ACIS system lacked FIM until after the breach had been discovered.[47]

Second, Equifax's web servers only retained log files back 30 days, whereas the National Institute of Standards and Technology recommended that companies retain logs going back at least three months (and up to a year, in some cases). Log files recorded activity on a network, allowing investigators to go back after a suspected breach and identify precisely what systems and information were compromised. They also made it easier to determine how hackers gained access to a network, enabling security professionals to more quickly eliminate vulnerabilities and backdoors. Information security experts had found that "targeted advanced attacks" on the networks of companies in the financial sector were only detected after, on average, 98 days, so maintaining log files for at least that much time was seen as crucial.[48]

Third, Equifax did not have a process in place for ensuring that SSL certificates throughout its systems were consistently up-to-date. At the time of the breach, Equifax was midway through rolling out a new SSL certificate management system that would have tracked the status of SSL certificates on the company's network across applications, enabling a regular scan of the entire network for expired certificates. Until that point, however, responsibility for maintaining each individual SSL certificate had lay with the individual IT staff member responsible for the relevant application. This had led to a substantial backlog of expired certificates.[49]

Many of Equifax's expired SSL certificates were part of "SSL visibility appliances" (SSLVs), which, when active, monitored encrypted traffic in and out of Equifax's network. These appliances were set up to continue to allow through-traffic even when they could not monitor it due to expired certificates. As a result, once the ACIS system's SSLV certificate expired in 2016, Equifax had no ability to monitor web traffic in or out of ACIS until after the breach. This meant that when in July 2017, cybersecurity experts started trying to determine how much damage the hackers had done, they lacked the records of server activity necessary to figure it out. Equifax knew of this vulnerability in their systems as early as January of 2017, when an internal security record was created stating: "SSLV devices are missing certificates, limiting visibility to web based attacks," but the problem nonetheless went unaddressed. In mid-2017, there were at least 324 expired SSL certificates across Equifax's network, and 79 of them were located in systems "monitoring highly business critical domains."[50]

In addition, once the hackers had infiltrated Equifax's system via the ACIS portal, they were able to move freely across its network "to any other device, database, or server . . . globally," because the servers that hosted the ACIS system were not segmented from the rest of Equifax's network. Though Equifax claimed to Senate investigators this was a deliberate choice to increase operational efficiency, the Senate investigation concluded that for the system to function properly, it would only have

required connections to three external databases. Instead, it was connected to a far larger number. Mauldin admitted to the House Committee that appropriate segmentation would have reduced the severity of the data breach, and both she and Payne further confessed that they had been unaware of the lack of segmentation until after the breach had been uncovered.[51]

The servers also permitted users to access sensitive administrator and configuration files from outside of the system. Like the lack of segmentation, the House investigation found this to be a substantial departure from consensus best practices in cybersecurity. As the House report explained, "If Equifax had limited access to sensitive files across its systems, the attackers may not have found the stored application credentials used to access sensitive databases outside the ACIS environment."[52]

Equifax's Breach Announcement and Response

On September 7, 2017, Equifax publicly announced that it had suffered a data breach exposing personal information on 143 million Americans (see **Exhibit 3** for Equifax's initial press release and **Exhibit 4** for a comparison of breach disclosure delays across companies). Equifax announced that it had established a website to help consumers determine if they were affected by the breach and that it had engaged Mandiant to help it assess the impact of the attack.[53] Smith said, "While we've made significant investments in data security, we recognize we must do more. And we will."[54] Equifax's stock price fell from a high of $143 before the breach announcement on September 7th to $93 about week later on September 15th, a decline of about 35 percent.

That same day, news broke that Equifax's Chief Financial Officer (CFO), president of U.S. information solutions, and president of workforce solutions had sold around $1.8 million worth of stock on August 1 and 2. A spokeswoman for Equifax said the three had no knowledge of the breach.[55]

Equifax took several steps to protect consumers affected by the breach, including: "1) credit file monitoring by all three credit bureaus; 2) Equifax credit lock; 3) Equifax credit reports; 4) identity theft insurance; and 5) Social Security Number 'dark web' scanning for one year."[56] These services, part of Equifax's TrustedID Premier service, were made available to all U.S. consumers for free for one year.[57]

Despite the company's efforts, Equifax's breach response exhibited significant missteps. For instance, after the company set up a website providing information about the breach with a unique domain: equifaxsecurity2017.com, a web developer created a similar-looking site at securityequifax2017.com to illustrate the security risk posed by unique domain. This confused even Equifax's official Twitter account, which directed consumers to the fake website (see **Exhibits 5** and **6** for the real and mocked up Equifax security websites).[58]

The website itself had a number of issues. A report prepared by the Office of Senator Elizabeth Warren found:

> 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 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.[59]

Consumers were also frustrated by the difficulty of contacting Equifax. Immediately following the breach, the company had around 500 customer service representatives on staff, forcing it to quickly

hire an additional 2,000 in the month after the announcement.[60] The Consumer Financial Protection Bureau (CFPB) reported over 7,500 complaints in the two months that followed relating to dropped calls, lengthy hold times, and Equifax agents not returning calls.[61]

Controversy even surrounded the company's offer of free credit file monitoring and identity theft protection. This service was provided by TrustedID, which Equifax owned. Critics complained that the service was only free for the first year; after that, consumers would be charged if they didn't call TrustedID to cancel their subscription. Critics were further incensed that the protection offer required those who signed up to agree to a mandatory, binding arbitration clause that precluded them from suing Equifax, including as part of class action lawsuits for damages caused by the breach (see **Exhibit 7** for text of the initial arbitration clause).[62] The clause sparked an uproar from consumers and others, including the New York State Attorney General, who complained that the terms of service were "unacceptable and unenforceable."[63] In response, Equifax added an explanation to the "frequently asked questions" section on its breach website on Friday, September 8, noting that the arbitration clause applied "to the free credit file monitoring and identity theft protection products, and not the cybersecurity incident."[64] Equifax eventually backtracked and removed the offending clause, claiming it had been included by mistake after the terms of use were copied from elsewhere.[65]

Besides the arbitration clause, Equifax also spurred outrage by initially charging consumers for credit freezes, which prevent credit bureaus from sharing a consumer's credit file with third parties with whom the consumer did not have a preexisting relationship. Equifax dropped the $30.95 fee after public outcry, providing credit freezes for free, but planned to drop the freezes in 2018 with the introduction of a new "credit lock" product. These moves led to criticism of the limited timeframes on Equifax's consumer protection measures. Consumers, the argument went, would be at risk of identity theft for years due to the exfiltration of their data, whereas Equifax was only providing them with free tools to prevent identity theft for the next year.[66]

Each day seemed to bring more public revelations about the extent of the breach. Although Equifax had initially claimed that hackers breached its systems in mid-May, public reports surfaced on September 18 detailing the initial breach in March (see **Exhibit 8** for a timeline of the Equifax breach).[67] Equifax claimed that there was no connection between the March breach and the May breach.[68] On October 2, Equifax confirmed that Mandiant's investigation had discovered an additional 2.5 million people effected by the breach.[69] On October 10, Equifax announced that ten million people had had driver's license data stolen[70] and that 700,000 U.K. customers had had information stolen.[71] In February 2018, reports emerged that the compromised consumer information had included passport numbers, which Equifax had not previously disclosed.[72]

Meanwhile, the identity and motive of the attacking group remained a mystery. Some investigators suspected that a foreign government was ultimately responsible for the breach based on its similarity to recent cyber-attacks at the health insurance provider Anthem, Inc. and the U.S. Office of Personnel Management. However, uncertainty remained, as Mandiant indicated in a report to Equifax clients in mid-September that it did not have enough data to identify those responsible.[73]

The Board of Directors and Its Role in Cybersecurity

Equifax's board faced significant scrutiny in the wake of the breach. The board had 11 members (see **Exhibit 9** for Equifax's board) with an average tenure of 9.3 years, above the S&P 500 average of 8.2 years, with one director who had served since 1992.[74] Among the three credit reporting agencies, Equifax was the only one with a separate technology committee mandated to monitor cybersecurity (see **Exhibit 10** for the charter of Equifax's technology committee). The technology committee would

"review the Company's technology investments and infrastructure associated with risk management, including policies relating to information security disaster recovery, and business continuity." It had five members and was chaired by John A. McKinley, CEO of senior care service provider SaferAging Inc. McKinley had previously served as CTO of News Corporation, AOL Technologies, Merrill Lynch, and GE Capital Corporation.[75] Another member, Mark Templeton, had recently served as CEO of networking software company Citrix Systems.

Fallout

In addition to the steep decline in the company's stock price, the breach also cost several executives their jobs. Equifax's CSO and CIO resigned on September 15.[76] Smith resigned as CEO and chairman on September 26 and was replaced by do Regos Barros as interim CEO and director Mark Feidler as non-executive chairman.[77]

Equifax's board reacted to charges of insider trading by the three executives who sold stock in the days after the breach was discovered and to allegations of malfeasance by the company's senior management. The board announced that it was considering clawing back compensation from Smith and Mauldin.[78] It also formed a special committee to review the stock sales and Kelley's role as CLO in approving them.[79] On October 26, the board announced that it was adding Scott McGregor, former CEO of semiconductor maker Broadcom, as a director, with Feidler saying that McGregor had "extensive data security, cybersecurity, information technology and risk management experience."[80] A few weeks later, on November 3, the board completed its review of the stock sales, finding that the executives in question did not know about the breach when they made their trades.[81]

The breach also led to dozens of lawsuits and government inquiries. The New York State Attorney General announced on September 11 that he had launched a formal investigation.[82] The Federal Trade Commission launched its own investigation on September 14,[83] and the Massachusetts Attorney General filed a lawsuit on September 19,[84] with the San Francisco City Attorney following on September 27.[85]

One U.S. senator called the Equifax breach "one of the most egregious examples of corporate malfeasances since Enron."[86] Another launched an investigation into the breach, sending letters to Equifax and the two other major credit reporting agencies, as well as to several U.S. government agencies.[87] Public officials were especially critical of Equifax's lack of transparency and its delay in notifying the public.[88] A group of senators introduced the Freedom from Equifax Exploitation Act, which would "enhance fraud alert procedures and provide free access to credit freezes, and for other purposes."[89]

The breach had the potential to completely change the operations of the credit reporting industry. The director of the CFPB said that the three main reporting agencies would face a "new regime" of regulation, with embedded regulators at each company to prevent further breaches of PII. Said the director, "There has to be a scheme of preventive monitoring in place. They're going to have to accept that, they're going to welcome that, they're going to have to be very forthcoming."[90]

On October 18, Change to Win (CtW) Investment Group, an investment advisor and shareholder activism group affiliated with CtW, a federation of U.S. unions representing 5.5 million members, sent a letter to Equifax chairman Mark Feidler criticizing the board:

> Despite being in the business of collecting, storing, and commercializing personal data, the haphazard response to the data breach indicates that the Board of Directors did not anticipate a core concern to the Company's operations. In doing so, it appears as though the Board and management gave little thought to preserving Equifax's most important asset—its reputation as a credit reporting agency.[91]

CtW asserted that Equifax's board "neglected to grasp the materiality of the data breach to both consumers and its shareholders. The group presented Equifax's board with six proposals to improve governance and hold executives accountable, including the removal of the chairmen of the audit and technology committees, permanently separating the CEO and chairman positions, and considering legal settlements in determining executive compensation (see **Exhibit 11** for the full list of CtW's proposals). CtW threatened to withdraw support the reelection of directors at Equifax's next annual meeting should Equifax fail to implement the proposals.[92]

Breach Disclosure Issues

The breach brought longstanding criticisms of U.S. data breach disclosure laws back to surface. About six weeks elapsed between when Equifax first discovered the breach and when the company first disclosed the breach to consumers. In the aftermath of the breach, observers questioned whether Equifax had violated any disclosure laws by waiting that long. Disclosure requirements, however, differed from state to state. In some states, disclosure was required within 45 days of discovery, while in others, no specific deadline was imposed, merely that companies notify consumers "as soon as possible." Some congressional representatives proposed bills that would create a unified 30-day timeframe for alerting consumers. Some states also sought to hold Equifax to stricter disclosure requirements, with New York working to apply its financial institution cybersecurity rules to credit reporting agencies, requiring them to alert state regulators of a breach within 72 hours of discovery.[93]

Conclusion

In the quarter following the breach announcement, Equifax's profits fell by 27 percent year-over-year. It immediately faced nearly $90 million in breach-related costs, 240 consumer lawsuits, separate investigations by the FTC, CFPB, SEC, and British and Canadian regulators, and requests for information about the breach from all 50 U.S. state attorneys general.[94] The damage to the company had been severe. Equifax, however, was not alone in suffering from malicious cyber activity. Over the course of 2017, the FBI received reports of data breaches from 3,785 different corporate victims across the U.S.[95] Furthermore, the IT company Cisco found that 55 percent of the 3,548 organizations it surveyed for its 2018 Security Capabilities Benchmark Study had experienced data breaches in 2017, as had 80 percent of organizations with over 50 vendors.[96] Moreover, hacks at large companies were generally not trivial. The President's Council of Economic Advisers found that on average, large cap, publicly traded corporations lost $498 million in market capitalization per major cyberattack they suffered between January 2000 and January 2017.[97] In light of this, while many experts asked what Equifax could have done differently to protect itself, others wondered whether Equifax was really negligent or just unlucky.

Exhibit 1 Technical Explanation of Hack Prepared by the House of Representatives Committee on Oversight and Government Reform

After entering the ACIS environment through the Apache Struts vulnerability, the attackers uploaded the first web shells, which are malicious scripts uploaded to a compromised server to enable remote control of the machine […]. Web shells can enable file system and database manipulation, facilitate system command execution, and provide file upload/download capability. In essence, a web shell provides a secret backdoor for an attacker to reenter and interact with a compromised system.

The ACIS environment was comprised of two web servers and two application servers, with firewalls set up at the perimeter of the web servers. Attackers exploited the Apache Struts vulnerability found on the application servers to bypass these firewalls. Once inside the network, the attackers created web shells on both application servers. This provided the attackers with the ability to execute commands directly on the system hosted on the application servers. Approximately 30 unique web shells were used to perform the attack. According to Mandiant, file integrity monitoring could have discovered the creation of these web shells by detecting and alerting to potentially unauthorized network changes. Equifax did not have file integrity monitoring enabled on the ACIS system at the time of the attack.

After installing the first web shells, the attackers accessed a mounted file share containing unencrypted application credentials (i.e., username and password) stored in a configuration file database […]. Mounting is a process by which the operating system makes files and directories on a storage device available for internal access via the computer's file system. Attackers were able to access the file share because Equifax did not limit access to sensitive files across its internal legacy IT systems. Ayres stated storage of these credentials in this manner was inconsistent with Equifax policy.

Although the ACIS application required access to only three databases within the Equifax environment to perform its business function, the ACIS application was not segmented off from other, unrelated databases. As a result, the attackers used the application credentials to gain access to 48 unrelated databases outside of the ACIS environment.

Attackers ran approximately 9,000 queries on these databases and obtained access to sensitive stored data […]. The attackers queried the metadata from a specific table to discover the type of information contained within the table. Once the attackers found a table with PII, they performed additional queries to retrieve the data from the table.184 In total, 265 of the 9,000 queries the attackers ran within the Equifax environment returned datasets containing PII. None of the PII contained in these datasets was encrypted at rest.

The attackers stored the PII data output from each of the 265 successful queries in files. The attackers compressed these files and placed them into a web accessible directory. Then, the attackers issued commands through the tool Wget – a common system utility that allows the user to issue commands and retrieve content from web servers – to transfer the data files out of the Equifax environment. The attackers used the web shells to exfiltrate some of the data […]. The attackers used an estimated 35 different IP addresses to interact with the ACIS environment.

Source: United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 31-33, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

Exhibit 2 Cybersecurity at Equifax and its Competitors

	TransUnion	Experian	Equifax
Deployment Time for Critical Patches	<14 days	<15 days	<2 days
Regular Vulnerability Scans	Weekly	Weekly	Monthly (and as needed)
Complete IT Asset Inventory	Yes	Yes	No
Verification Process for Patch Installation	Yes	Yes	No
Official Policy for Tracking SSL Certificate Validity	No	No	No

Source: United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 5, 35-36, 55-62 https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

Exhibit 3 Equifax Press Release Announcing Data Breach, September 7, 2017

Equifax Inc. (NYSE: EFX) today annouced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes 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. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also 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."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559,

which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.

Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."

Source: "Equifax Announces Cybersecurity Incident Involving Consumer Information." Equifax, Inc., September 7, 2017, https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628, accessed October 2017.

Exhibit 4 Timing of Disclosure of Major Data Breaches

Company	Year of Breach	Time Between Discovery and Disclosure
Home Depot	2014	6 days
Target	2013	7 days
Anthem	2015	8 days
Google	2018	~7 months
Yahoo	2013	~3 years
Equifax	2017	~6 weeks

Source: United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 46-51, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

Exhibit 5 Equifax Data Breach Homepage, eqiufaxsecurity2017.com, September 8, 2017.

Source: equifaxsecurity2017.com, accessed via archive.org, January 2018.

Exhibit 6 Fake Equifax Data Breach Homepage, securityequifax2017.com

Source: Dell Cameron, "Equifax Has Been Sending Consumers to a Fake Phishing Site for Almost Two Weeks." Gizmodo, September 20, 2017.

Exhibit 7 Text of Initial TrustedID Arbitration Clause

ARBITRATION. PLEASE READ THIS ENTIRE SECTION CAREFULLY BECAUSE IT AFFECTS YOUR LEGAL RIGHTS BY REQUIRING ARBITRATION OF DISPUTES (EXCEPT AS SET FORTH BELOW) AND A WAIVER OF THE ABILITY TO BRING OR PARTICIPATE IN A CLASS ACTION, CLASS ARBITRATION, OR OTHER REPRESENTATIVE ACTION. ARBITRATION PROVIDES A QUICK AND COST EFFECTIVE MECHANISM FOR RESOLVING DISPUTES, BUT YOU SHOULD BE AWARE THAT IT ALSO LIMITS YOUR RIGHTS TO DISCOVERY AND APPEAL.

Except as otherwise expressly provided in this Agreement, all claims, disputes, or controversies raised by either You or TrustedID, Inc. arising from or relating to the subject matter of this Agreement or the Products ("Claim" or "Claims") shall be finally settled by arbitration in the county (or parish) where you live or where You and TrustedID, Inc. otherwise agree using the English language in accordance with the Arbitration Rules and Procedures of JAMS then in effect, by one commercial arbitrator with substantial experience in resolving complex commercial contract disputes, who may or may not be selected from the appropriate list of JAMS arbitrators.

This arbitration will be conducted as an individual arbitration. Neither You nor We consent or agree to any arbitration on a class or representative basis, and the arbitrator shall have no authority to proceed with arbitration on a class or representative basis. No arbitration will be consolidated with any other arbitration proceeding without the consent of all parties. This class action waiver provision applies to and includes any Claims made and remedies sought as part of any class action, private attorney general action, or other representative action. By consenting to submit Your Claims to arbitration, You will be forfeiting Your right to bring or participate in any class action (whether as a named plaintiff or a class member) or to share in any class action awards, including class claims where a class has not yet been certified, even if the facts and circumstances upon which the Claims are based already occurred or existed.

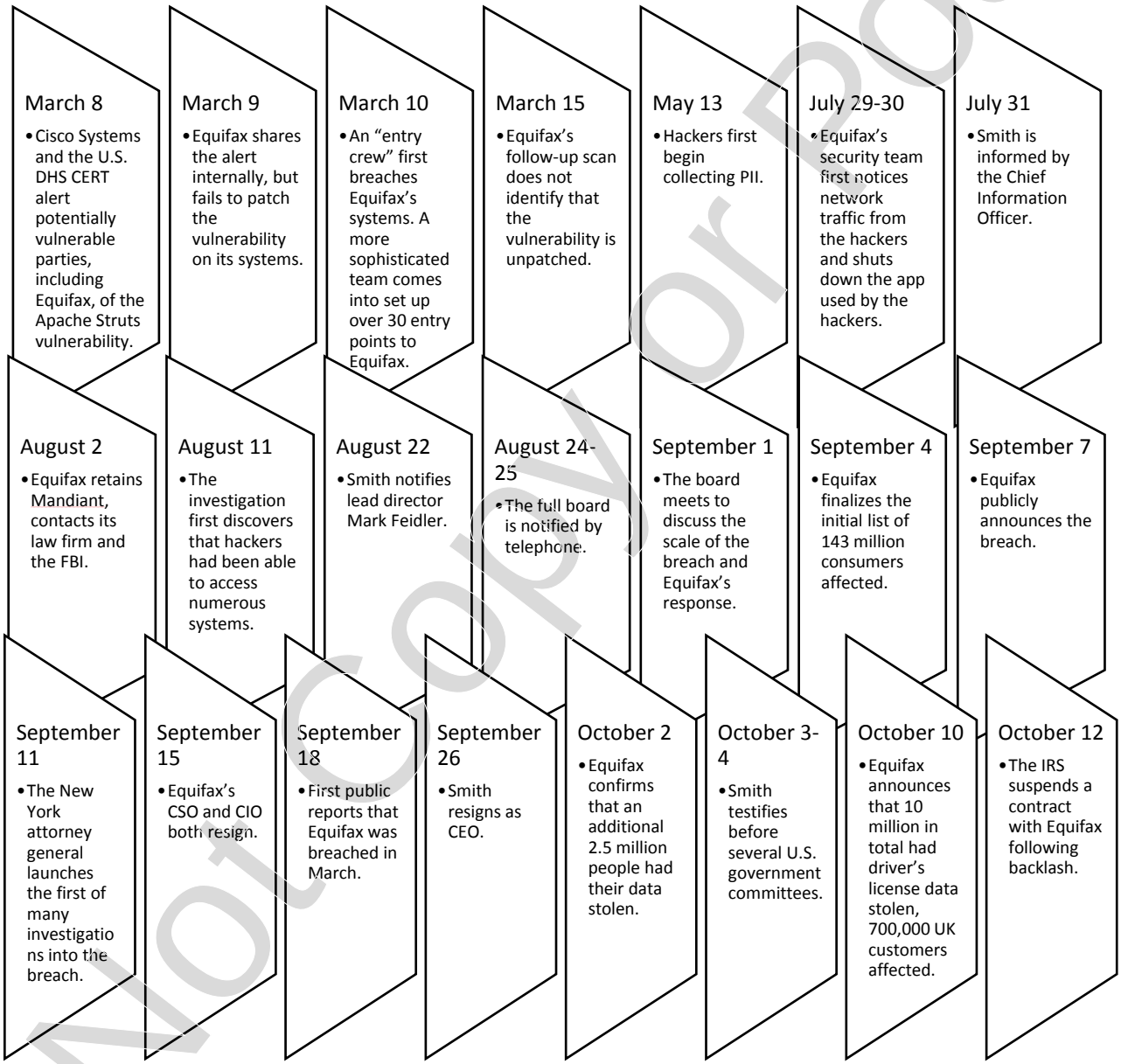
…

Notwithstanding anything in this Section, either You or TrustedID, Inc. may bring an individual action in small claims court as long as (i) the claim is not aggregated with the claim of any other person, and (ii) the small claims court is located in the same county (or parish) and state as Your address that You most recently provided to TrustedID, Inc. according to TrustedID, Inc.'s records in connection with this Agreement.

Source: Equifax Terms of Use as Of September 6, 2017, accessed via https://web.archive.org/web/20170909011235/https://www.trustedid.com/premier/terms-of-use.php, January 2018.

Note: The arbitration clause was initially included in the Terms of Use when consumers signed up for free protection from Equifax's TrustedID product. The clause was removed on September 8, 2017.

Exhibit 8 Timeline of Equifax Data Breach



Source: Compiled by casewriters.

Exhibit 9 Equifax's Board of Directors

Name	Director Since	Biography
Robert D. Daleo	2006	Retired vice chairman of Thomson Reuters and a board member at Citrix Systems. Previously the executive vice president and CFO of Thomson Reuters.
Walter W. Driver, Jr.	2007	Chairman- Southeast of Goldman, Sachs & Co and director at Total System Services, Inc. Previously the chairman of King & Spalding LLP.
Mark L. Feidler*	2007	Founding partner of Msouth Equity Partners and lead director at New York Life Insurance Company. Previously president and COO of BellSouth Corporation and COO of Cingular Wireless.
G. Thomas Hough*	2016	Former Americas vice chair of Ernst & Young LLP. Board member at Publix Super Markets Inc. and Federated Fund Family. Hough spent his entire career in Ernst & Young.
L. Phillip Humann	1992	Retired executive chairman of the board of SunTrust Banks, Inc. Humann was previously chairman and CEO of SunTrust Banks, as well as president of the company. Presiding director at Coca-Cola Enterprises, Inc. and lead director at Haverty Furniture Companies, Inc.
Robert D. Marcus	2013	Non-executive chairman at Ocelot Partners Limited. Former chairman and CEO of Time Warner Cable Inc. from 2014-2016, where he had served in various positions since 1998. Practiced law at Paul, Weiss, Rifkind, Wharton & Garrision prior to his time at Time Warner.
Siri S. Marshall	2006	Former senior vice president, general counsel, secretary, and chief governance and compliance officer at General Mills, Inc. Director at Ameriprise Financial, Inc., and former director at Alphatec Holdings, Inc., and BioHorizons, Inc.
John A. McKinley*	2008	CEO at SaferAging, Inc and co-founder of venture capital firm LaunchBox Digital. Former CTO of News Corporation, AOL Technologies, Merrill Lynch, and GE Capital Corporation. Also served as president of AOL digital services.
Richard F. Smith	2005	Chairman and CEO of Equifax. Served as COO of GE Insurance Solutions and president and CEO of GE Property and Casualty Reinsurance. Also served as president and CEO of GE Capital Fleet Services.
Elane B. Stock*	2017	Former group president, Kimberly-Clark International and director at YUM! Brands, Inc. Served in various senior leadership positions at Kimberly-Clark, as well as national vice president of strategy for the American Cancer Society and regional manager Georgia-Pacific's Color-Box division.
Mark B. Templeton*	2008	Former CEO, president, and director of Citrix Systems, Inc, where he served as CEO from 1999–2015.

Source: 2017 Proxy Statement. Equifax, Inc., March 24, 2017.

Note: An asterisk (*) denotes membership of the technology committee. John A. McKinley served as the chair of the technology committee. Richard Smith served as chairman and CEO until his resignation on September 26, at which time Mark Feidler was appointed chairman. The board appointed former Broadcom CEO Scott McGregor to the board on October 26, 2017.

Exhibit 10 Charter for Equifax's Technology Committee

I. Purpose

The purpose of the Technology Committee is to review and monitor the Company's technology strategy and significant technology investments in support of its evolving global business needs. Areas of review include: information technology strategy; significant new product lines or technology investments; and the Company's response to external technology-based threats and opportunities. In addition, the Committee will oversee the Company's mitigation of any identified enterprise-wide risks in the above areas.

II. Members

The Committee shall consist of three or more directors appointed annually by the Board of Directors, and may include the Chairman of the Board and Chief Executive Officer. The following skills are particularly useful for the Committee members to have: familiarity and experience with technology products, development and marketing, and technology risk assessment.

III. Meetings

… The Committee will report its activities and findings to the Board on a regular basis.…

IV. Responsibilities and Duties

The goals and responsibilities of the Committee are to monitor the Company's long-term strategy and significant investments in the areas listed below… The intervals for review of any given policy or program may be annual, biannual, or at longer or shorter intervals, depending upon the nature of the subject matter and developments affecting the Company with respect to that subject matter.

1. Information technology long-term strategy in support of the Company's evolving global business needs.

2. Review and present observations to the Board with respect to the annual technology budget.

3. Significant new product development programs (including software initiatives) and new technology investments, including technical and market risks associated with product development and investment.

4. Future trends in technology that may affect the Company's strategic plans, including overall industry trends and new opportunities and threats occasioned by new technologies, especially disruptive technologies.

5. Review the Company's technology investments and infrastructure associated with risk management, including policies relating to information security, disaster recovery and business continuity.

6. Assess the scope and quality of the Company's intellectual property.

7. Undertake from time to time such additional activities within the scope of the Committee's primary purposes as it may deem appropriate and/or as assigned by the Board of Directors, the Chairman of the Board and Chief Executive Officer.

Source: Excerpted from: Committee Charters. Equifax, Inc., http://www.equifax.com/about-equifax/corporate-governance/committee-charters, accessed October 2017.

Exhibit 11 Change to Win Investment Group's Proposals for Equifax's Board

- Permanently separate the CEO and Chairman positions to provide better Board oversight of management.
- Replace the Chairman of the Audit Committee, Robert Daleo, and Chairman of the Technology Committee, John McKinley, as the directors with the responsibilities most germane to the current crisis and the Company's inadequate response.
- Revise the Company's clawback policy to allow the Board to recoup executive compensation for financial and reputational damage to the Company based not only on executive misconduct, but also supervisory failures, with disclosure to shareholders of any recoupment.
- Include legal claims, settlements, and costs related to the data breach in performance measures used to determine executive compensation.
- Have the Special Committee of directors formed in response to the data breach (a) evaluate the financial impact of the breach on the Company, (b) review the Company's cybersecurity response plans, and (c) ensure that any future breaches are escalated to the Board level. The Company should also disclose to shareholders the Committee's findings.
- Establish a multi-stakeholder advisory council specializing in data security and composed of outside issue-area experts and stakeholder advocates to address the public policy concerns related to the Company's data security practices

Source: Letter to Richard F. Smith, Former Chairman and Chief Executive Officer, Equifax. Senator Elizabeth Warren, October 12, 2017.

Endnotes

[1] "Company Profile." Equifax, http://www.equifax.com/about-equifax/company-profile, accessed October 13, 2017.

[2] This paragraph derives from: 2016 Annual Report. Equifax, Inc., February 22, 2017.

[3] Ibid.

[4] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 17, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; "Equifax Inc. (NYSE: EFX) Transaction Summary > M&A/Private Placements," S&P Capital IQ, accessed April 2019.

[5] Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros." Bloomberg Businessweek, September 29, 2017; "Richard (Rick) F Smith, Advisor (Current), Equifax Inc," BoardEx, accessed April 2019.

[6] "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information." Office of Senator Elizabeth Warren, February 2018.

[7] Paragraph derives from: Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros." Bloomberg Businessweek, September 29, 2017; "Anthony (Tony) W Spinelli, COO/Division President (Current), Fractal Industries Inc," BoardEx, accessed April 2019.

[8] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 7, 19, 61-62, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 35, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[9] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 62, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[10] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 62, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[11] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 7, 19, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[12] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 36-43, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019; United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 64-65, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[13] Paragraph derives from: Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros." Bloomberg Businessweek, September 29, 2017.

[14] Lorenzo Franceschi-Bicchierai, "Equifax Was Warned." Vice, October 26, 2017.

[15] Paragraph derives from: AnnaMaria Andriotis and Robert McMillan, "Equifax Security Showed Signs of Trouble Months Before Hack." Wall Street Journal, September 26, 2017.

[16] Equifax Inc. ESG Ratings Report. MSCI, Last updated February 16, 2018.

[17] Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros." Bloomberg Businessweek, September 29, 2017.

[18] AnnaMaria Andriotis and Robert McMillan, "Hackers Entered Equifax Systems in March." Wall Street Journal, September 20, 2017.

[19] Paragraph derives from: Dan Goodin, "Critical vulnerability under "massive" attack imperils high-impact sites [Updated]." Ars Technica, March 9, 2017.

[20] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 8, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[21] Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017.

[22] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 2, 27, 29, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[23] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 29, 64-65, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[24] Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017.

[25] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 37-40, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[26] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 41-43, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[27] Paragraph derives from: Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros." Bloomberg Businessweek, September 29, 2017.

[28] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 43-45, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019; United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 70-71, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[29] Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 46, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[30] Paragraph derives from: Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017.

[31] "Equifax Announces Cybersecurity Incident Involving Consumer Information." Equifax, Inc., September 7, 2017.

[32] Tara Siegel Bernard and Stacy Cowley, "Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says." New York Times, October 3, 2017.

[33] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 52, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[34] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 52, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[35] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 52, 63, 67, 71, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 36, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[36] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 52, 63, 66-67, 71, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[37] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 60-61, 69-74, 79-80, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[38] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 68-70, 76, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 22-23, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[39] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 25-27, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[40] United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 25, 28, 30, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[41] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 7, 55-57, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[42] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 58, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[43] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 60, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[44] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 59-60, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[45] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 61-62, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[46] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 71-72, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[47] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 77, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[48] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 78-79, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019

[49] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 33-34, 70, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 43-44, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[50] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 33-35, 70, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 43-45, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[51] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 73, 76-77, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019; United States Senate: Committee on Homeland Security and Government Affairs, "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, March 2019, p. 45-46, https://www.carper.senate.gov/public/_cache/files/5/0/508a6447-853f-4f41-85e8-1927641557f3/D5CFA4A0FC19997FF41FB3A5CE9EB6F7.equifax-report-3.6.19.pdf, accessed March 2019.

[52] United States House of Representatives: Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, December 2018, p. 77-78, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf, accessed January 2019.

[53] "Equifax Announces Cybersecurity Incident Involving Consumer Information." Equifax, Inc., September 7, 2017.

[54] "Equifax Announces Cybersecurity Incident Involving Consumer Information." Equifax, Inc., September 7, 2017.

[55] Anders Melin, "Three Equifax Managers Sold Stock Before Cyber Hack Revealed." Bloomberg, September 7, 2017.

[56] Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017.

[57] "Equifax Announces Cybersecurity Incident Involving Consumer Information." Equifax, Inc., September 7, 2017.

[58] Dell Cameron, "Equifax Has Been Sending Consumers to a Fake Phishing Site for Almost Two Weeks." Gizmodo, September 20, 2017.

[59] "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information." Office of Senator Elizabeth Warren, February 2018.

[60] Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017.

[61] "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information." Office of Senator Elizabeth Warren, February 2018.

[62] Paragraph derives from: AnnaMaria Andriotis and Aaron Luchetti, "Consumers Blast Equifax's Hack Response. Wall Street Journal, September 8, 2017.

[63] Andrew Blake, "Equifax updates terms of service after arbitration clause causes uproar following massive breach." The Washington Times, September 9, 2017.

[64] AnnaMaria Andriotis and Aaron Lucchetti, "Consumers Blast Equifax's Hack Response." Wall Street Journal, September 8, 2017.

[65] Prepared Testimony of Richard F. Smith. Richard Smith, October 4, 2017.

[66] Paragraph derives from: "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information." Office of Senator Elizabeth Warren, February 2018.

[67] Michael Riley, Anita Sharpe, and Jordan Robertson, "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed." Bloomberg, September 18, 2017.

[68] Michael Riley, Anita Sharpe, and Jordan Robertson, "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed." Bloomberg, September 18, 2017.

[69] Stacy Cowley, "2.5 Million More People Potentially Exposed in Equifax Breach." New York Times, October 2, 2017.

[70] AnnaMaria Andriotis and Emily Glazer, "Equifax Hack Disclosed Driver's License Data for More Than 10 Million Americans." Wall Street Journal, October 10, 2017.

[71] Caroline Binham, "Equifax says nearly 700,000 UK customers may have had details stolen in hack." Financial Times, October 10, 2017.

[72] "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information." Office of Senator Elizabeth Warren, February 2018.

[73] Paragraph derives from: Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros." Bloomberg Businessweek, September 29, 2017.

[74] Stephen Gandel, "Equifax Board Needs a Security Dream Team." Bloomberg Gadfly, September 21, 2017.

[75] Notice of 2017 Annual Meeting and Proxy Statement. Equifax, Inc., March 24, 2017, p. 14.

[76] Jennifer Surane and Anders Melin, "Equifax CEO Richard Smith Resigns After Uproar Over Massive Hack." Bloomberg, September 26, 2017.

[77] Jennifer Surane and Anders Melin, "Equifax CEO Richard Smith Resigns After Uproar Over Massive Hack." Bloomberg, September 26, 2017.

[78] Emily Glazer and AnnaMaria Andriotis, "Equifax Board Considers Clawing Back Executives' Compensation; Directors have been discussing best approach for clawbacks." Wall Street Journal, September 29, 2017.

[79] Elizabeth Dexheimer, "Equifax Forms Panel to Review Executives' Share Sales." Bloomberg, September 29, 2017; AnnaMaria Andriotis and Emily Glazer, "At the Center of the Equifax Mess: Its Top Lawyer." Wall Street Journal, October 1, 2017.

[80] "Equifax Names Scott McGregor as New Independent Director." Equifax, October 26, 2017.

[81] "Equifax Board Releases Findings of Special Committee Regarding Stock Sale by Executives." Equifax, November 3, 2017.

[82] Jaclyn Jaeger, "New York AG launches formal investigation into Equifax breach." Compliance Week, September 11, 2017.

[83] Dustin Volz and Susan Heavey, "FTC probes Equifax; top Democrat likens it to Enron." Reuters, September 14, 2017.

[84] AnnaMaria Andriotis, "Massachusetts Attorney General Hits Equifax With Suit Over Hack." Wall Street Journal, September 19, 2017.

[85] Sarah Buhr, "San Francisco sues Equifax on behalf of 15 million Californians affected by the breach." Techcrunch, September 27, 2017.

[86] Dustin Volz and Susan Heavey, "FTC probes Equifax; top Democrat likens it to Enron." Reuters, September 14, 2017.

[87] "Warren Launches Investigation into Equifax Breach with Letters to Equifax, TransUnion, Experian, FTC, CFPB, GAO." Office of Senator Elizabeth Warren press release, September 15, 2017.

[88] "Warren Launches Investigation into Equifax Breach with Letters to Equifax, TransUnion, Experian, FTC, CFPB, GAO." Office of Senator Elizabeth Warren press release, September 15, 2017.

[89] Freedom from Equifax Exploitation Act. September 15, 2017, p. 1.

[90] Paragraph derives from: Jeff Cox, "Big changes coming for credit firms in wake of Equifax hack, CFPB director says." CNBC, September 27, 2017.

[91] Letter to Equifax chairman Mark Feidler. Dieter Waizenegger, Executive Director of Change to Win Investment Group, October 18, 2017.

[92] Paragraph derives from: Letter to Equifax chairman Mark Feidler. Dieter Waizenegger, Executive Director of Change to Win Investment Group, October 18, 2017.

[93] Paragraph derives from: Michael Rapoport and AnnaMaria Andriotis, "States Push Equifax to Explain Why It Took 6 Weeks to Disclose Hack." Wall Street Journal, October 28, 2017.

[94] Derives from: Stacy Cowley, "Equifax Faces Mounting Costs and Investigations From Breach." New York Times, November 9, 2017.

[95] "2017 Internet Crime Report," Federal Bureau of Investigation Internet Crime Complaint Center, May 7, 2018, p. 20, https://pdf.ic3.gov/2017_IC3Report.pdf, accessed April 2019.

[96] "Cisco 2018 Annual Cybersecurity Report," Cisco Systems, Inc., February 6, 2018, p. 50-51, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf, accessed April 2019.

[97] Kevin A. Hassett, Richard V. Burkhauser, and Tomas J. Philipson, "The Annual Report of the Council of Economic Advisers," Council of Economic Advisers, Executive Office of the President, February 21, 2018, p. 333-334, https://www.whitehouse.gov/wp-content/uploads/2018/02/ERP_2018_Final-FINAL.pdf, accessed April 2019.