How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Rob Portman, Chairman
Tom Carper, Ranking Member

HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH

TABLE OF CONTENTS

HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH

EXECUTIVE SUMMARY

The effects of data breaches are often long-lasting and challenging to reverse. Victims who have had their sensitive personal or financial information stolen by hackers can be left with years of expense and hassle. No type of entity or sector of the economy has been immune to data breaches. In 2018 alone, Google+, Facebook, Ticketfly, T-Mobile, Orbitz, Saks, Lord & Taylor, and Marriott all announced significant breaches. The importance of protecting personally identifiable information ("PII") grows with every successive data breach.

Consumers and businesses are well aware of the need to safeguard items like driver's licenses, credit cards, and financial records that criminals can use to their advantage. Consumers also understand the need to protect information like online passwords, pin numbers, and Social Security numbers. But a consumer taking appropriate care of this information may not be enough to keep PII out of the hands of criminal hackers. In the modern world, businesses collect and compile data about their customers and potential customers. Without proper precautions, this information can be stored or transmitted in ways that leave it vulnerable to theft.

The information collected by consumer reporting agencies ("CRAs") to compile credit reports is one example of PII that must be protected. This information includes a consumer's name, nicknames, date of birth, Social Security number, telephone numbers, and current and former addresses. Credit reports also typically include a list of all open and closed credit accounts, account balances, account payment histories, and the names of creditors. The information tells the story of a consumer's financial life and can determine whether they can rent an apartment, buy a car, or qualify for a home loan. If stolen, criminals can use it to do significant financial harm. The steps CRAs take to safeguard consumers' credit histories are extremely important. If that information is compromised, consumers should know to be on heightened alert to monitor their finances and mitigate any potential damage.

In 2017, one of the largest CRAs, Equifax Inc. ("Equifax") announced that it had suffered a data breach that involved the PII of over 145 million Americans. The Subcommittee investigated the causes of this breach to identify ways to prevent future incidents of this scope. The Subcommittee also reviewed the efforts of Equifax's two largest competitors, Experian plc ("Experian") and TransUnion LLC ("TransUnion"), in responding to the vulnerability that ultimately led to the Equifax data breach. Highlights of the Subcommittee's investigative results, including findings and recommendations, are provided below.

Equifax Failed to Prioritize Cybersecurity. Equifax had no standalone written corporate policy governing the patching of known cyber vulnerabilities until 2015. After implementing this policy, Equifax conducted an audit of its patch management efforts, which identified a backlog of over 8,500 known vulnerabilities that had not been patched. This included more than 1,000 vulnerabilities the auditors deemed critical, high, or medium risks that were found on systems that could be accessed by individuals from outside of Equifax's information technology ("IT") networks. The audit report concluded, among other things, that Equifax did not abide by the schedule for addressing vulnerabilities mandated by its own patching policy. It also found that the company had a reactive approach to installing patches and used what the auditors called an "honor system" for patching that failed to ensure that patches were installed. The audit report also noted that Equifax lacked a comprehensive IT asset inventory, meaning it lacked a complete understanding of the assets it owned. This made it difficult, if not impossible, for Equifax to know if vulnerabilities existed on its networks. If a vulnerability cannot be found, it cannot be patched.

Equifax never conducted another audit after the 2015 audit and left several of the issues identified in the 2015 audit report unaddressed in the months leading up to the 2017 data breach.

Equifax Could Not Follow Its Own Policies in Patching the Vulnerability That Ultimately Caused the Breach. Equifax's patching policy required the company's IT department to patch critical vulnerabilities within 48 hours. The company's security staff learned of a critical vulnerability in certain versions of Apache Struts – a widely-used piece of web application software – on March 8, 2017, from the U.S. Computer Emergency Readiness Team at the U.S. Department of Homeland Security. The National Institute of Standards and Technology gave the vulnerability the highest criticality score possible; it was widely known that the vulnerability was easy to exploit. Equifax employees circulated news of the vulnerability through an internal alert the next day that went to a list of more than 400 company employees.

Equifax held monthly meetings to discuss cyber threats and vulnerabilities, but senior managers did not routinely attend these meetings and follow-up was limited. The Apache Struts vulnerability was discussed during the March 2017 and April 2017 meetings, but not discussed at any subsequent monthly meetings. The Subcommittee interviewed the leadership of the Equifax IT and security staffs and learned that none of them regularly attended these monthly meetings or specifically recalled attending the March 2017 meeting. In addition, the Chief Information Officer ("CIO"), who oversaw the IT department during 2017, referred to patching as a "lower level responsibility that was six levels down" from him.

Equifax Failed to Locate and Patch Apache Struts. The Equifax developer who was aware of Equifax's use of Apache Struts software was not included in the 400-person email distribution list used to circulate information on the vulnerability. The developer's manager, however, was on the distribution list and received the alert, but failed to forward it to the developer or anyone on the developer's team. As a result, the key developer never received the alert. Equifax added application owners to the list after the breach.

The Subcommittee also learned that Equifax developers were individually responsible for subscribing to push notifications from software vendors about security vulnerabilities. The developer who knew of the company's use of Apache Struts software was not subscribed to notifications from Apache and did not receive any alerts about the vulnerability.

On March 14, 2017 – nearly a week after the Apache Struts vulnerability was disclosed – Equifax added new rules to the company's intrusion prevention system intended to help it thwart efforts to exploit the vulnerability. With these new protections in place, Equifax believed it had the ability to identify and block exploit attempts and did block several attempts the same day the rules were installed.

None of Equifax's subsequent scans identified the vulnerable version of Apache Struts running on Equifax's network. And since Equifax lacked a comprehensive inventory of its IT assets, it did not know that the vulnerable version of Apache Struts remained on its system.

Equifax Left Itself Open to Attack Due to Poor Cybersecurity Practices. Equifax was unable to detect attackers entering its networks because it failed to take the steps necessary to see incoming malicious traffic online.

Website owners install Secure Sockets Layer ("SSL") certificates to protect and encrypt online interactions with their servers. If an SSL certificate expires, transactions are no longer protected. As part of an IT management effort unrelated to the Apache Struts vulnerability, Equifax installed dozens of new SSL certificates on the night of July 29, 2017, to replace certificates that had expired. This included a new certificate for the expired SSL certificate for its online dispute portal. The SSL certificate needed to be up-to-date to properly monitor the online dispute portal, but had expired eight months earlier in November 2016. Almost immediately after updating the SSL certificate, company employees observed suspicious internet traffic from its online dispute portal that they were able to trace to an IP address in China, a country where Equifax does not operate. After blocking the IP address, Equifax observed similar traffic the following day to another IP address that appeared to be connected to a Chinese entity and decided to take the online dispute portal offline. Equifax later determined that the hackers first gained

access to Equifax's system through the online dispute portal on May 13, 2017, meaning the hackers had 78 days to maneuver undetected.

Equifax confirmed to the Subcommittee that the Apache Struts vulnerability facilitated the data breach that began in May 2017.

The Damage Done by the Hackers Could Have Been Minimized. Once inside Equifax's online dispute portal, the hackers also accessed other Equifax databases as they searched for other systems containing PII. They eventually found a data repository that also contained unencrypted usernames and passwords that allowed the hackers to access additional Equifax databases. The information accessed primarily included names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license and credit card numbers.

The usernames and passwords the hackers found were saved on a file share by Equifax employees. Equifax told the Subcommittee that it decided to structure its networks this way due to its effort to support efficient business operations rather than security protocols.

In addition, Equifax did not have basic tools in place to detect and identify changes to files, a protection which would have generated real-time alerts and detected the unauthorized changes the hackers were making.

Equifax Waited Six Weeks Before Notifying the Public It Was Breached. Equifax employees discovered the suspicious activity that was later determined to be a data breach on July 29, 2017. Equifax's then-Chief Executive Officer, Richard Smith, learned of the breach on July 31 and that consumer PII maintained by Equifax had likely been stolen on August 15, 2017. Mr. Smith waited until August 22 to begin notifying members of Equifax's Board of Directors. Equifax publicly announced the data breach on September 7, *six weeks after* learning of it and *nearly four months after* the hackers entered Equifax's networks. Because Equifax was unaware of all the assets it owned, unable to patch the Apache Struts vulnerability, and unable to detect attacks on key portions of its network, for months consumers were unaware that criminals had obtained their most sensitive personal and financial information and that they should take steps to protect themselves from fraud. Equifax officials say the company chose to notify the public only after determining every single individual impacted by the breach.

There is no national uniform standard requiring a private entity to notify affected individuals in the event of a data breach. Instead, all 50 states, the District of Columbia, and several U.S. territories have enacted their own legislation requiring public disclosure of security breaches of PII. Some states require notification after any breach of non-encrypted personal information, while others require notification only if the breach is likely to cause "substantial harm" to

individuals. Some states require companies to notify affected individuals within a set number of days, while others simply require private entities to provide notice "without unreasonable delay." This creates a patchwork of uncertainty for companies and consumers responding to data breaches. For example, Target, one of the largest retail chains in the United States, notified the public seven days after learning that it suffered a data breach. By contrast, Yahoo! suffered data breaches in 2013 and 2014, but did not disclose them until 2016 and 2017, respectively.

Equifax Executives Believe They Did All They Could to Prevent the Breach. The Subcommittee interviewed current and former Equifax employees from the information security and IT departments. Their responses varied, but most said they believe that the security team's actions were an appropriate response to the Apache Struts vulnerability. The Director of Global Threats and Vulnerability Management from 2014 to 2017 said "security wasn't first" at Equifax before the data breach, but that the data breach "made everyone focus on it more." The former Countermeasures Manager in place from 2016 to 2017 said he believes the response to the vulnerability was "not only defensible, but justifiable." The CIO at Equifax from 2010 to 2017 oversaw the company employees responsible for installing patches but said he was never made aware of the Apache Struts vulnerability and does not understand why the vulnerability "was not caught." He does not think Equifax could have done anything differently.

TransUnion and Experian Avoided a Breach. TransUnion and Experian received the same information as the public and Equifax regarding the Apache Struts vulnerability, but the approach that each company took to cybersecurity was different from Equifax's. Both companies had deployed software to verify the installation of security patches, ran scans more frequently, and maintained an IT asset inventory. In response to the Apache Struts vulnerability, TransUnion began patching vulnerable versions of the software within days. Experian retained a software security firm in March 2017 to conduct targeted vulnerability scans of Apache Struts vulnerabilities. After finding an Experian server was running a vulnerable version, Experian took the server offline and began patching it. There is no indication that TransUnion or Experian were attacked by hackers seeking to exploit the Apache Struts vulnerability.

Equifax Failed to Preserve Key Internal Chat Records. Equifax was unable to produce potentially responsive documents related to the data breach because the company failed to take steps to preserve records created on an internal chat platform. Equifax's document retention policy requires the company to preserve several types of documents for different periods of time. In general, Equifax employees are required to preserve all business records, unless they are considered "disposable" under the policy. The policy also gives the Equifax legal department the authority to halt the disposal of any records that are subject to a legal hold due to litigation or a government investigation.

During its investigation, the Subcommittee learned that Equifax employees conducted substantive discussions of the discovery and mitigation of the data breach using Microsoft Lync, an instant messaging product. Equifax's policy was that records of these chats were disposable. As such, Equifax maintained the default setting on the chat platform not to archive chats. After discovering the data breach on July 29, 2017, Equifax did not issue a legal hold for related documents until August 22, 2017. Despite the legal hold, Equifax did not change the default setting on the Lync platform and begin archiving chats until September 15, 2017. As a result, the Subcommittee does not have a complete record of documents concerning the breach.

The Subcommittee's Investigation

The Subcommittee initiated an investigation into the circumstances surrounding the Equifax cybersecurity breach, which was announced on September 7, 2017. The Subcommittee later expanded its scope to include a review of the steps taken by two of Equifax's largest competitors, Experian and TransUnion, in responding to an identified cybersecurity vulnerability that facilitated the Equifax breach. As part of the investigation, the Subcommittee reviewed over 45,000 pages of documents from Equifax, Experian, and TransUnion. The Subcommittee also conducted numerous witness interviews and received briefings from key personnel at all three companies, as well as cybersecurity experts in the federal government and private industry. All entities cooperated with the Subcommittee's requests for information, briefings, and interviews on a voluntary basis.

Based on this investigation, the Subcommittee concludes that Equifax's response to the March 2017 cybersecurity vulnerability that facilitated the breach was inadequate and hampered by Equifax's neglect of cybersecurity. Equifax's shortcomings are long-standing and reflect a broader culture of complacency toward cybersecurity preparedness. The Subcommittee also lacks a full understanding of the breach, as the company failed to preserve relevant messages sent over an internal messaging platform.

Findings of Fact and Recommendations

Findings of Fact

(1) Equifax Suffered a Data Breach in 2017. On September 7, 2017, Equifax announced that the company suffered a data breach impacting over 145 million Americans. On October 2, 2017, Equifax revised its initial estimate to include an additional 2.5 million Americans for a total of 145.5 million. A vulnerability in Apache Struts – a widely used web application development software – facilitated the breach. The

hackers who exploited this vulnerability were able to gain access to the Equifax online dispute portal and then other internal company databases.

(2) Equifax Learned of Significant Cybersecurity Deficiencies in 2015. An internal patch management audit report from 2015, concerning efforts at Equifax to update computer assets to address known security issues, concluded that "current patch and configuration management controls are **not** adequately designed to ensure Equifax systems are securely configured and patched in a timely manner." Several current and former Equifax employees were dismissive of the *number* of vulnerabilities identified by the audit. The 2015 audit identified more than 8,500 vulnerabilities that Equifax employees failed to address for more than 90 days beyond the recommended patching timeframe. This list included more than 1,000 externally facing vulnerabilities rated as critical, high, or medium.

(3) Equifax Lacked a Comprehensive Information Technology ("IT") Asset Inventory. The 2015 audit highlighted Equifax's lack of a complete inventory of the company's IT assets, including the software applications in use. The lack of an IT asset inventory limited the effectiveness of scanning tools and other processes used to identify and remediate known cybersecurity vulnerabilities. For example, when the U.S. Department of Homeland Security ("DHS") provided notification that Apache Struts contained a critical vulnerability, Equifax had no inventory to determine where or if it used Apache Struts on its network.

(4) Equifax Used What Internal Auditors Called an "Honor System" for Patching Vulnerabilities. At the time of the 2017 breach, Equifax had no formalized method of validating the successful installation of patches. The 2015 audit referred to this approach as an "honor system" in which the IT team responsible for installing patches would notify the security team once installation was complete. The security team would then scan the systems that were patched to determine if patch installation was successful. If a scan did not reveal a vulnerability, the security team assumed that a patch was successfully applied or that a vulnerability did not exist.

(5) Equifax Conducted No Follow-Up Audit After the Findings of the 2015 Audit. In August 2017, the Senior Vice President of Equifax's Internal Audit Group informed Equifax's Chief Security Officer ("CSO") that the audit team had "not done a formal follow-up" to the 2015 report. None of the individuals the Subcommittee

interviewed could recall Equifax conducting another patch management audit during their tenure with the company.

(6) The Apache Struts Vulnerability That Led to the Breach in March 2017 Was Widely Known. The DHS U.S.-Computer Emergency Readiness Team ("US-CERT") sent a public alert on March 8, 2017 after learning of the vulnerability and the National Institute of Standards and Technology ("NIST") assigned the highest possible severity score, a 10, to it. Members of Equifax's cybersecurity team received the US-CERT alert on the same day. On March 9, 2017, Equifax's Global Threats and Vulnerability Management ("GTVM") team circulated the US-CERT notice to more than 400 Equifax employees. However, a developer who used Apache Struts did not receive the notice, which instructed those responsible for running Apache Struts applications to upgrade to recommended safer versions of the software.

(7) The Tools Necessary to Exploit the March 2017 Apache Struts Vulnerability Were Publicly Available and Easy to Use. The exploit code for the Apache Struts vulnerability and accompanying instructions were available online four days before Apache released a patch to address the vulnerability. Without the patch, individuals with basic computer skills – not just skilled hackers – could follow published instructions and exploit the vulnerability.

(8) Equifax Was Unable to Meet the Timeline in Its Patch Management Policy in Responding to the Apache Struts Vulnerability. Equifax's patch management policy identifies schedules for the installation of patches, based upon the criticality of the vulnerability each patch addresses. According to Equifax's policy, the IT team must install critical patches within 48 hours, or in the timeframe agreed upon with the security team. A March 9, 2017, email from the GTVM team noted that the Apache Struts vulnerability required patching within 48 hours. Equifax did not patch the Apache Struts vulnerability until August 2017 because it was unable to detect a vulnerable version of Apache Struts on the system due to a lack of a comprehensive IT asset inventory.

(9) Equifax Only Discussed the Apache Struts Vulnerability in Its March and April 2017 Meetings on Threats and Vulnerabilities. Equifax holds monthly meetings led by the GTVM team to discuss the latest cybersecurity threats. The March 2017 GTVM PowerPoint presentation listed the Apache Struts vulnerability as an agenda item, and the team discussed it during a meeting on March 16, 2017. The

April 2017 GTVM PowerPoint presentation also referenced the Apache Struts vulnerability twice. No further discussion of the Apache Struts vulnerability appears to have taken place at any subsequent GTVM monthly teams meetings prior to the discovery of the July 2017 breach.

(10) Senior Managers from Equifax Security Teams Did Not Regularly Participate in GTVM Meetings. Most of the senior managers interviewed by the Subcommittee who oversaw various Equifax cybersecurity teams in 2017 did not recall attending the GTVM meeting on March 16, 2017, during which GTVM discussed the Apache Struts vulnerability. They also did not recall whether they received a summary of the meeting from any colleagues or subordinates. These managers also indicated they typically did not personally participate in these monthly meetings. Members of Equifax's Senior Leadership Team, including the then-CSO, also did not regularly attend GTVM meetings. Equifax had no policy governing who must attend GTVM meetings and inconsistently tracked participation.

(11) The Key Equifax Employee Aware of the Use of Apache Struts Was Not Included on the GTVM Email Distribution List and Did Not Receive the March 2017 Alert. Equifax's internal developer of the online dispute portal, the hacked application, was aware that the company's network used versions of Apache Struts, but was not on the alert distribution list that included 400 Equifax employees. This developer did not receive notice of the vulnerability in March 2017, and therefore took no action to make others aware of the online portal's use of Apache Struts. Equifax added application owners to the list after the breach.

(12) Equifax Scanned Its Systems and Servers for the Vulnerable Versions of Apache Struts and Found No Threat. Equifax regularly scans its network for known vulnerabilities. In response to news of the Apache Struts vulnerability, Equifax performed a scan intended to identify attempts to exploit vulnerable versions of Apache Struts. Equifax engaged its scanning tool repeatedly but did not search at the appropriate network levels and, thus, did not identify the vulnerable version of Apache Struts. This was due, in part, to Equifax's failure to maintain a comprehensive IT asset inventory. Without this inventory, Equifax was unable to direct its scanning tools precisely to search for the Apache Struts vulnerability.

(13) Expired Secure Sockets Layer ("SSL") Certificates Delayed Equifax's Ability to Detect the Breach for Months. SSL

certificates must be active to allow a website to decrypt and monitor incoming network traffic. The SSL certificate for the Equifax online dispute portal expired in November 2016 and was not updated for another eight months after that date. Equifax first observed suspicious activity from its online dispute portal on July 29, 2017, after updating the expired SSL certificate for that application**.** Equifax traced the IP address for the activity to a location in China. Equifax does not conduct any business in China, and as a result, immediately blocked the IP address. Equifax took its online dispute portal offline on July 30, 2017, after observing additional suspicious activity from an IP address connected to a Chinese entity. It was later determined the hackers first accessed Equifax's system on May 13, 2017 – 78 days before Equifax discovered the breach.

(14) Once Inside Equifax's Online Dispute Portal, the Hackers Accessed Other Equifax Systems. After gaining access to Equifax's online dispute portal, the attackers attempted to pull sensitive information from other Equifax databases. These efforts led the hackers to a data repository containing personally identifiable information ("PII"), along with unencrypted usernames and passwords for numerous other databases. These databases contained the PII for approximately 145 million American consumers. Access to this information was possible due to Equifax's decision not to segment its systems by restricting unnecessary access to other systems once a user was inside the dispute portal. This was a decision by Equifax to support efficient business operations and functionality, but it was inconsistent with a standard recommended in the NIST cybersecurity framework.

(15) Current and Former Equifax Employees Interviewed by the Subcommittee Believed Equifax Acted Appropriately in Responding to the March 2017 US-CERT Alert Regarding the Apache Struts Vulnerability. Current and former Equifax employees from the cybersecurity team independently expressed their views to Subcommittee staff that their team's response to the Apache Struts vulnerability was appropriate and justified.

(16) Equifax Waited Six Weeks to Notify the Public of the Breach in September 2017. Equifax employees first discovered suspicious activity that was later determined to be a breach on July 29, 2017. The company's then-Chief Executive Officer, Richard Smith, was informed on July 31 that the security team had discovered a security incident and taken down the online dispute portal. Mr. Smith was informed on August 15, 2017, that it appeared consumer PII had likely

been stolen. Equifax did not make a public announcement until September 7, 2017, six weeks after learning of the security incident.

(17) Equifax's Largest Competitors, TransUnion and Experian, Quickly Identified Vulnerable Versions of Apache Struts and Proactively Installed the Patch. While all three major consumer reporting agencies ("CRAs") had similar policies on vulnerability scanning and patching, TransUnion and Experian had an accurate and updated IT asset inventory, which they used to identify and track applications and software across their entire network. This allowed TransUnion and Experian to identify which applications on their networks were using vulnerable versions of Apache Struts. Once they identified the vulnerable applications, each company took steps to patch the applications in an effort to prevent a data breach.

(18) Equifax Failed to Properly Preserve All Documents Related to the Breach. Several current and former Equifax employees stated that they regularly used an internal chat system, Microsoft Lync, to communicate with other Equifax employees throughout the company. These individuals told the Subcommittee they used Microsoft Lync to communicate real-time findings related to the breach once they discovered the suspicious activity. They also told the Subcommittee they used Lync to discuss subsequent response efforts. While the company's document retention policy defines a "record" to include any document written in the course of company business, Equifax considers these Lync types of chats to be disposable records. While the legal hold was issued on August 22, 2017, Equifax did not begin to preserve Lync chats until September 15, 2017. Therefore, the Subcommittee does not have a complete record of documents concerning the breach.

Recommendations

(1) Congress should pass legislation that establishes a national uniform standard requiring private entities that collect and store PII to take reasonable and appropriate steps to prevent cyberattacks and data breaches. Several cybersecurity recommendations, including a widely known framework from NIST, already exist. However, the framework is not mandatory, and there is no federal law requiring private entities to take steps to protect PII.

(2) Congress should pass legislation requiring private entities that suffer a data breach to notify affected consumers, law enforcement, and the appropriate federal regulatory agency without unreasonable delay. There is no national uniform

standard requiring a private entity to notify affected individuals in the event of a data breach. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring data breach notification laws. In the absence of a national standard, states have taken significantly different approaches to notification standards with different triggers for notifications and different timelines for notifying individuals whose information has been stolen or improperly disclosed.

(3) Congress should explore the need for additional federal efforts to share information with private companies about cybersecurity threats and disseminate cybersecurity best practices that IT asset owners can adopt. Several federal agencies have released materials discussing information sharing for cyber threats. In addition, there are dozens of Information Sharing and Analysis Centers ("ISACs") and Information Sharing and Analysis Organizations across several industries, sectors, and regions in the United States. However, participation in an ISAC is voluntary, formal meetings are rare, and ISACs are funded by members.

(4) Federal agencies with a role in ensuring private entities take steps to prevent cyberattacks and data breaches and protect PII should examine their authorities and report to Congress with any recommendations to improve the effectiveness of their efforts.

(5) Private entities should re-examine their data retention policies to ensure these policies properly preserve relevant documents in the event of a cyberattack. An incomplete record regarding how an attack occurred, what the attacker damaged or stole, and how a company responded to the attack can hinder efforts by law enforcement to investigate and prosecute attackers and prevent policymakers and enforcement agencies from taking steps to prevent future incidents.

I. BACKGROUND

Private companies and government agencies all work to defend their IT networks against hackers and criminals online. They devote substantial resources to these efforts, spending significant sums of money on hardware, software, and skilled IT personnel deployed to prevent unauthorized access to their systems and the theft of sensitive and proprietary data.[1] They have also taken steps to share

[1] Jonathan Vanian, *Here's How Much Businesses Worldwide Will Spend on Cybersecurity by 2020*, FORTUNE (Oct. 12, 2016), http://fortune.com/2016/10/12/cybersecurity-global-spending.

more information on cybersecurity threats with industry and government partners and to work together to adapt their cybersecurity tactics to the ever-evolving threats they face.[2] While all entities that operate IT systems have a shared goal of preventing cyberattacks and data breaches, there are ongoing debates about the best way to prevent them – and also how and when to notify the public when information is compromised.[3]

The costs to entities suffering data breaches and the individuals whose PII is disclosed as a result of a breach can be both financial and reputational.[4] No type of entity or sector of the economy has been immune to data breaches. In the last decade alone, private companies across a range of industries such as Yahoo!, Target, Sony's PlayStation network, eBay, Uber, and Anthem have all experienced data breaches, which collectively impacted billions of individuals.[5] Nor are government agencies immune. The U.S. Office of Personnel Management suffered a widely publicized data breach in 2014 that allowed hackers to obtain millions of extremely sensitive federal personnel records.[6] Most recently, on November 30, 2018, Marriott International, Inc. announced a data breach impacting as many as 383 million guests of Starwood Hotels and Resorts.[7]

In 2017, Equifax Inc. ("Equifax"), one of the three largest CRAs, suffered a data breach that compromised the personal information of over 145 million Americans.[8] Equifax's data breach prompted the Subcommittee to launch an investigation into the causes of and circumstances surrounding the breach. As part of this investigation, the Subcommittee reviewed the cybersecurity policies and procedures in place at Equifax prior to and at the time of the breach. The Subcommittee also reviewed Equifax's response to the specific vulnerability that led to the breach and sought to understand how two of Equifax's biggest competitors, Experian plc ("Experian") and TransUnion LLC ("TransUnion"), avoided suffering a

---

[2] *Report Incidents, Phishing, Malware, or Vulnerabilities*, US-CERT, https://www.us-cert.gov/report.
[3] Gloria Gonzalez, *Congress Urged to Adopt National Data Breach Standard*, BUS. INS. (Feb. 14, 2018), https://www.businessinsurance.com/article/20180214/NEWS06/912319215/Congress-urged-to-adopt-national-data-breach-standard.
[4] *Identity Theft*, U.S DEP'T OF JUST., https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud; Ransomware: The Attacker's Choice for Cyber Extortion, FireEye, https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html.
[5] Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, CSO (Dec. 20, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.
[6] *What Happened*, U.S. OFF. PERSON. MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents.
[7] Patricia Clark, *Marriott Says Only 383 Million Guests Exposed in Breach*, BLOOMBERG (Jan. 4, 2019), https://www.bloomberg.com/news/articles/2019-01-04/marriott-lowers-estimate-to-383-million-guests-exposed-in-breach. *See also Marriott Announces Starwood Guest Reservation Database Security Incident*, MARRIOTT (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.
[8] Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People could be Affected*, CNN (Sept. 8, 2017), http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html.

data breach attributable to this same vulnerability. Overall, the Subcommittee reviewed over 45,000 pages of documents and conducted seven staff interviews and briefings with Equifax, Experian, TransUnion, and other relevant government agencies, including NIST. All entities complied with the Subcommittee's requests for documents and information.

A. Consumer Reporting Agencies

CRAs compile and sell credit reports on an individual's borrowing and loan repayment history.[9] Most consumers have a personal credit report from multiple CRAs.[10] Credit reports often contain personal information, such as an individual's name (including nicknames), date of birth, Social Security number, telephone numbers, and current and former addresses.[11] Credit reports also typically include credit account information, such as a list of all open and closed credit accounts, dates when each account was opened and closed, credit limits, account balances, account payment histories, and the names of creditors.[12] Credit reports may also contain relevant public records, including records involving foreclosures, civil suits and judgments, overdue child support, liens, and bankruptcy filings.[13] There are three major CRAs operating in the United States: Equifax, Experian, and TransUnion.[14]

The information held by these three companies – private entities with operations around the world – provides the primary criteria by which a consumer's creditworthiness is judged. According to the Consumer Financial Protection Bureau ("CFPB"), "banks, credit unions, retail credit card issuers, auto lenders, mortgage lenders, debt collectors, and others voluntarily send information to credit reporting companies."[15] Credit reports detailing personal credit histories and the credit scores derived from the information in these reports can impact many aspects of consumers' lives.[16] Lenders often require a credit report before deciding whether to

---

[9] Companies that assemble consumer credit information and sell this information are referred to as "consumer reporting agencies" by the legislation governing credit reports. *See* Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified at 12 U.S.C. §§ 1681-1681x (2012)). These companies can also be referred to as "credit bureaus," "credit reporting companies," or "credit reporting agencies."

[10] *What Is a Credit Report?*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-report-en-309.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] BD. OF GOVERNORS OF THE FED. RESERVE SYS., CONSUMERS GUIDE: CREDIT REPORTS AND CREDIT SCORES, https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf.

[15] *How Do Credit Reporting Companies Get My Information?*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/ask-cfpb/how-do-credit-reporting-companies-get-my-information-en-1263.

[16] *What Is a Credit Report?*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-report-en-309.

offer various forms of credit to a consumer.[17] Other businesses use credit reports to determine whether to offer insurance coverage, rent a dwelling, or provide various forms of utility services.[18] Some employers also use credit reports to make employment decisions.[19] Credit reports and credit scores also help determine the interest rates offered on mortgages, automobiles, and other consumer loans.[20]

1. Equifax

Equifax was incorporated in Georgia in 1913, though its predecessor company dates back to 1899.[21] Equifax offers products and services to financial institutions, corporations, governments, and individual consumers.[22] Equifax maintains comprehensive databases of consumer and business information derived from various sources.[23] The company analyzes this information to help develop decision-making solutions and processing services for its clients.[24]

Headquartered in Atlanta, Georgia, Equifax operates or has investments in 24 countries across four global regions: North America, Asia Pacific, Europe, and Latin America.[25] Equifax employs 10,400 employees worldwide.[26] Equifax organizes, assimilates, and analyzes data on more than 820 million consumers and more than 81 million businesses, and its database includes employee data contributed from more than 7,100 employers.[27]

2. Experian

In 1996, the company known today as Experian was sold to another company based in the United Kingdom after initially entering the credit reporting industry in the United States in 1968.[28] Experian's clients include financial services organizations and entities in the retail, catalog, telecommunications, utility, media,

---

[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] EQUIFAX, 2017 ANNUAL REPORT 2 (2018), https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2017-annual-report.pdf.
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Company Profile*, EQUIFAX, https://www.equifax.com/about-equifax/company-profile.
[26] *Id.*
[27] Gary Strauss, *How to Protect Your Personal Data from Hackers*, AARP (Sept. 8, 2017), https://www.aarp.org/money/scams-fraud/info-2017/equifax-cyber-attack-data-breach-fd.html; *Communications, Utilities, and Digital Media*, EQUIFAX, https://www.equifax.com/business/communications-utilities-and-digital-media/.
[28] NIGEL WATSON, A BRIEF HISTORY OF EXPERIAN 10, 20 (2013), https://www.experianplc.com/media/1323/8151-exp-experian-history-book_abridged_final.pdf.

insurance, automotive, leisure, e-commerce, manufacturing, property, and government sectors.[29]

Experian's corporate headquarters are in Dublin, Ireland, but the company has corporate offices around the world, including in the United States.[30] Altogether, Experian employs 16,500 people in 39 countries.[31] It maintains credit information on approximately 220 million U.S. consumers and 40 million active U.S. businesses.[32]

3. TransUnion

TransUnion has maintained and updated information on virtually every consumer in the United States since 1988.[33] It entered the direct-to-consumer market in 2002 with the acquisition of TrueCredit.com, a company that offers individuals access to their credit report as well as credit monitoring services.[34] TransUnion has expertise in financial services, specialized risk, insurance, and healthcare.[35]

TransUnion is headquartered in Chicago, Illinois, and has offices in North America, Africa, Latin America, and Asia.[36] TransUnion employs nearly 4,000 employees in the United States and 7,100 employees globally.[37] It has a consumer credit database of 1 billion consumers in over 30 countries; a global customer base of over 65,000 businesses; and 90,000 data sources, including financial institutions, private databases, and public records repositories.[38]

B. Federal Regulation of Consumer Reporting Agencies

CRAs that operate in the United States are subject to numerous federal laws and regulations governing the collection, protection, and use of consumer credit and

---

[29] *Experian Announces New Global Image and Identity*, EXPERIAN, https://www.experianplc.com/media/news/2007/03-09-2007.
[30] *About Us*, EXPERIAN, https://www.experianplc.com/about-us.
[31] *Id.*
[32] Corporate Fact Sheet, EXPERIAN, https://www.experian.com/corporate/experian-corporate-factsheet.html.
[33] *Company History*, TRANSUNION, https://www.transunion.com/about-us/company-history.
[34] *Id.*
[35] TRANSUNION, 2017 ANNUAL REPORT 1 (2018), http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_TRU_2017.pdf.
[36] *Id.* at 18.
[37] TRANSUNION, FORM 10-K (FEB. 14, 2019), https://otp.tools.investis.com/clients/us/transunion/SEC/sec-show.aspx?Type=html&FilingId=13231168&CIK=0001552033&Index=10000.
[38] TRANSUNION, 2017 ANNUAL REPORT 1–2 (2018), http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_TRU_2017.pdf.

other related information.[39] The Federal Trade Commission ("FTC") and the CFPB are the two federal agencies with primary regulatory authority over CRAs. The FTC is an independent agency that works to prevent anticompetitive, deceptive, and unfair business practices.[40] Similarly, the CFPB "regulates the offering and provision of consumer financial products or services under the federal consumer financial laws and educates and empowers consumers to make better informed financial decisions."[41] The CFPB has also "begun exercising supervisory authority over certain larger participants in the credit reporting market."[42]

The Fair Credit Reporting Act ("FCRA") promotes the accuracy, fairness, and privacy of information in CRA files.[43] To ensure compliance, the FTC maintains an enforcement program aimed at the main players in the credit reporting system – CRAs, those who send CRAs information, and those who use the consumer reports CRAs create.[44] The FCRA limits the type of information that CRAs may report, restricts the distribution and use of consumer reports, and establishes consumer rights to access and dispute their credit files.[45] CRAs are required to follow reasonable procedures that promote the accurate collection of information relating to individual consumers.[46] If a consumer disputes the accuracy of any information in the consumer's file, CRAs must conduct a reasonable reinvestigation.[47] CRAs are also required to provide consumers with a free annual credit report.[48] The FCRA imposes many other requirements on CRAs, data furnishers, and users of consumer report information.[49] Violation of the FCRA can result in civil penalties.[50]

The CFPB enforces certain provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") applicable to CRAs.[51] These provisions prohibit unfair, deceptive, or abusive acts or practices with respect to consumer finance and provide enforcement authority to the CFPB.[52] For example, the CFPB may pursue administrative proceedings or litigation.[53] In these proceedings, the CFPB can obtain cease and desist letters, impose monetary

---

[39] *See infra* text accompanying notes 40-42.
[40] *About the FTC*, FED. TRADE COMM'N., https://www.ftc.gov/about-ftc.
[41] About Us, CONSUMER FIN. PROT. BUREAU., https://www.consumerfinance.gov/about-us/.
[42] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-559, ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 6 (2017); *See also* 12 C.F.R. § 1090.104(b) (2019).
[43] 15 U.S.C. § 1681 (2017).
[44] 15 U.S.C. § 1681s (2017); *Credit Reporting*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/consumer-finance/credit-reporting.
[45] 15 U.S.C. §§ 1681a–1681m (2017).
[46] 15 U.S.C. § 1681(b) (2017).
[47] 15 U.S.C. § 1681i(a)(1) (2017).
[48] 15 U.S.C. § 1681j(a)(1)(A) (2017).
[49] 15 U.S.C. §§ 1681–1681x (2017).
[50] 15 U.S.C. §§ 1681n–1681o, 1681s (2017).
[51] 12 U.S.C. § 5511(b) (2017).
[52] 12 U.S.C. §§ 5492(a), 5531(a) (2017).
[53] 12 U.S.C. §§ 5563(a), 5564 (2017).

penalties for ordinary and knowing violations, and pursue additional types of affirmative relief.[54] The CFPB also has the authority to examine and supervise CRAs.[55] Finally, the CFPB has authority to supervise the larger CRAs.[56]

CRAs are also subject to certain provisions of the Financial Services Modernization Act of 1999.[57] Specifically, CRAs must comply with provisions relating to the use or disclosure of the underlying data and rules relating to the physical, administrative, and technological protection of non-public personal financial information.[58] Failure to comply can result in civil or criminal liability and sanctions from regulatory entities.[59] There are several federal agencies that enforce these requirements, including the FTC.[60]

The FTC considers multiple factors in determining whether it should take enforcement action against companies that violate data security provisions.[61] For example, the FTC considers whether a company's data security measures are commensurate with the company's size.[62] Nevertheless, the FTC can rely on its enforcement authority only after an incident has occurred; it does not have proactive, supervisory authority to examine CRAs' compliance with the FTC Act.[63] In June 2015, the FTC released a security guide for businesses that details lessons learned from FTC enforcement cases.[64] The FTC has also released guidance for businesses to help them understand the voluntary NIST Cybersecurity Framework and how it complements FTC's own security guide for businesses.[65]

C. The Federal Government's Role in Sharing Information on Cybersecurity Threats

---

[54] 12 U.S.C. §§ 5563(b), 5565 (2017).
[55] 12 U.S.C. § 5515(b) (2017).
[56] 12 C.F.R. § 1090.104(b) (2019); *CFPB to Supervise Credit Reporting*, CONSUMER FIN. PROT. BUREAU (July 16, 2012), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-to-superivse-credit-reporting/.
[57] *See infra* text accompanying notes 58-60.
[58] 15 U.S.C. § 6801(b) (2017).
[59] 15 U.S.C. §§ 6821–23 (2017).
[60] 15 U.S.C. § 6805(a) (2017).
[61] *See infra* text accompanying note 62.
[62] *Commission Statement Marking the FTC's 50th Data Security Settlement*, FED. TRADE COMM'N (Jan. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-559, ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 7 (2018).
[63] 15 U.S.C. § 45(b) (2017); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-559, ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 7 (2017).
[64] FED. TRADE COMM'N. START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[65] FED. TRADE COMM'N. CYBERSECURITY FOR SMALL BUSINESS: UNDERSTANDING THE NIST CYBERSECURITY FRAMEWORK (2018), https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework.

US-CERT is an entity within DHS's National Cybersecurity and Communications Integration Center ("NCCIC").[66] US-CERT is responsible for "disseminating cyber threat warning information and coordinating incident response activities."[67] In that role, US-CERT aggregates and disseminates cybersecurity information intended to help recipients prevent and respond to cyberattacks.[68]

US-CERT has partnerships with private sector security vendors, academia, federal agencies, ISACs, state and local governments, and international organizations.[69] US-CERT has established several initiatives intended to facilitate information sharing and collaboration on cybersecurity issues across industry.[70] For example, companies can sign up for email alerts from US-CERT that provide timely information about current security issues, hardware and software vulnerabilities, and information on how these vulnerabilities can be exploited or patched.[71] These alerts are also distributed on the US-CERT website in a plain text news feed that individuals can sign up to follow.[72] The US-CERT Current Activity web page also has a regularly updated summary of the most frequent, high-impact security incidents of which US-CERT is currently aware.[73]

In carrying out its mission, US-CERT uses the Common Vulnerability Scoring System ("CVSS"), a system for assessing and assigning numerical scores to cyber vulnerabilities based on their severity.[74] The Forum of Incident Response and Security Teams, a non-profit organization representing cyber incident responders around the world, manages CVSS.[75] CVSS assigns a score from 1-10 to each vulnerability, with 10 being the most critical, and these numbers then determine the priority of vulnerability remediation activities.[76] NIST documents CVSS scores on its National Vulnerability Database.[77] US-CERT uses its email alerts and communications posted to its website to explain the criticality of newly-discovered vulnerabilities to companies and present steps they can take to address them.[78] It often does this through the dissemination of Common Vulnerabilities and

---

[66] *About Us,* US-CERT, https://www.us-cert.gov/about-us.
[67] *Info Sheet,* US-CERT, https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf.
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Mailing Lists and Feeds*, US-CERT, https://www.us-cert.gov/mailing-lists-and-feeds.
[72] *Alerts*, US-CERT, https://www.us-cert.gov/ncas/alerts.
[73] *Current Activity*, US-CERT, https://www.us-cert.gov/ncas/current-activity.
[74] *Common Vulnerability Scoring System SIG*, FIRST, https://first.org/cvss.
[75] *Id.*
[76] *Common Vulnerability Scoring System v.3.0: Specification Document*, FIRST, https://www.first.org/cvss/specification-document.
[77] *National Vulnerability Database: Vulnerability Metrics*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, https://nvd.nist.gov/vuln-metrics/cvss.
[78] About Us, US-CERT, https://www.us-cert.gov/about-us.

Exposures ("CVE"), each of which is listed on the NIST website with its own identification number, a brief description, and at least one public reference.[79]

D. Data Breach Notification Standards

There is no national uniform standard requiring a private entity to notify affected individuals in the event of a data breach. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring data breach notification laws.[80] While no two laws are identical, the majority of data breach laws include provisions regarding who must comply with the law, definitions of PII, definitions of what constitutes a breach, and requirements for notice to consumers.[81] In addition, some states have laws requiring breached entities to assist affected individuals in mitigating potential adverse effects, such as through the provision of credit monitoring services.[82]

Some state data breach laws require public disclosure of security breaches of information involving PII.[83] In the absence of a federal standard governing non-federal entities, states have taken significantly different approaches to notification standards, creating uncertainty for companies and consumers responding to data breaches. Some states, such as New York, require notification after any breach of non-encrypted personal information, while others, like Alabama, require notification only if the breach is likely to cause "substantial harm" to individuals.[84] Some states require companies to notify affected individuals within a certain time frame, such as 30 days (Florida), 45 days (Washington), or 60 days (Delaware) while others simply require companies to provide notice "without unreasonable delay" (California).[85] State laws also differ in how they define "personal information," whether and when companies must notify any state agencies, the required contents of the notice, and the required method of notice.[86]

---

[79] *See Newest CVE Entries*, COMMON VULNERABILITIES & EXPOSURES, https://cve.mitre.org.
[80] Security Breach Notification Laws, NAT'L CONF. OF ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[81] *Id.*
[82] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-559, ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 20 n.32 (2017).
[83] *Id.* at 18 n.30.
[84] N.Y. GEN. BUS. § 899-AA(d) (2018); N.Y. STATE TECH. § 208 (2018); Alabama Data Breach Notification Act of 2018, SB 318.
[85] FLA. STAT. § 501.171(3)(a) (2018); WASH. REV. CODE §§ 19.255.010(16), 42.56.590(15) (2018); DEL. CODE. ANN. tit. 6 § 12B-102(c) (2018); CAL. CIV. CODE § 1798.82(a) (2018).
[86] CHRIS D. LINEBAUGH, CONG. RESEARCH SERV., LSB10210, WHAT LEGAL OBLIGATIONS DO INTERNET COMPANIES HAVE TO PREVENT AND RESPOND TO A DATA BREACH? 3 (2018).

II. EQUIFAX WAS AWARE OF CYBERSECURITY WEAKNESSES FOR YEARS

A. Equifax Learned of Significant Cybersecurity Deficiencies in 2015

According to the former CSO of Equifax, prior to 2015, Equifax had no official corporate policy governing how to patch known cybersecurity vulnerabilities on company systems and there was no document clearly outlining responsibilities.[87] The former CSO recognized this deficiency and offered to assist in creating such a policy.[88] After the former CSO obtained the support of the then-Chief Information Officer ("CIO"), she implemented Equifax's Patch Management Policy in April 2015.[89] Once the policy was in place, Equifax conducted an internal audit of its configuration and patch management processes to assess their effectiveness and issued an internal report on the audit findings on October 28, 2015.[90]

1. Purpose of the Audit

According to the audit report, the purpose of the configuration and patch management audit was three-fold: 1) to assess the effectiveness of processes and controls in place for vulnerability, patch, and configuration management; 2) to assess the security of production networks by identifying high-risk vulnerabilities related to depreciated patches, configuration issues, running services, compromised patches, and configuration management that could be exploited to gain privileged access to Equifax's production environment; and 3) to make recommendations to improve the security of Equifax's production network.[91]

The report further defined vulnerability, patch, and configuration management. Vulnerability management, according to the report, is a continual process for "identifying, assessing, prioritizing, and remediating IT security vulnerabilities" to keep Equifax's networks safe, and not a one-time activity.[92] Patch management is the process of "applying updates to computer assets to address known security vulnerabilities."[93] Further, it noted, even if "one computer in the environment is not patched, it can threaten the stability of the entire

---

[87] Interview with the former Chief Security Officer, Equifax (Oct. 4, 2018) [hereinafter Former CSO Interview (Oct. 4, 2018)].
[88] *Id.*
[89] EFXCONG-PSI000000196–206. Counsel for Equifax stated that the company's 2013 Global Security Policy contained a section related to patch management. Equifax did not produce this document to the Subcommittee. Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019).
[90] Former CSO Interview (Oct. 4, 2018).
[91] EFXCONG-PSI000032255–63.
[92] EFXCONG-PSI000032257.
[93] *Id.*

environment."[94] Finally, the report defined configuration management as the process of "implementing and maintaining changes to network hardware and software."[95] On this subject, the report noted that "a well-defined configuration management process that integrates information security is needed" to ensure that any network configurations do not negatively impact information security.[96]

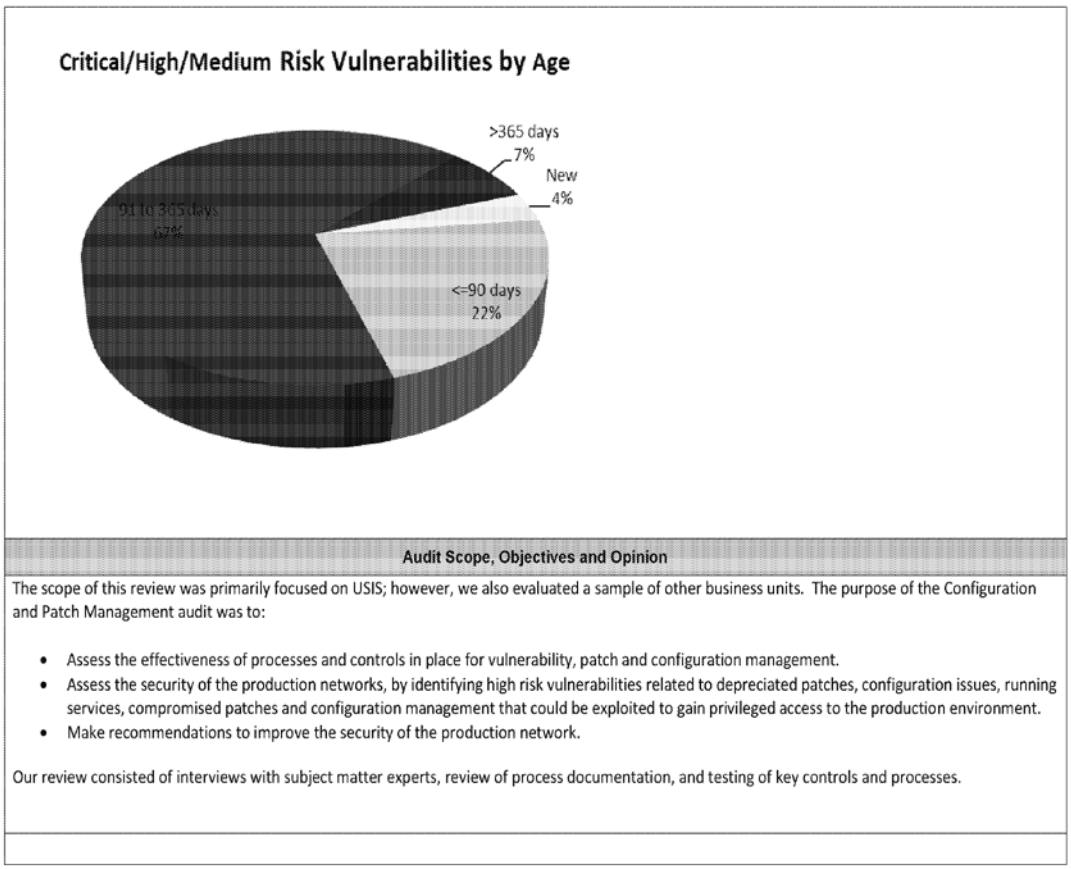
2. The Audit Highlighted a Backlog of over 8,500 Vulnerabilities with Overdue Patches

The audit report highlighted a number of deficiencies in the company's system controls. Specifically, the report noted that "current patch and configuration management controls are **not** adequately designed to ensure Equifax systems are securely configured and patched in a timely manner."[97]

According to the report, as of August 2015, there were "over **1000** [sic] known critical/high/medium vulnerabilities on externally facing systems (approximately 1150 [sic] hosts) and over **7500** [sic] critical/high vulnerabilities (not including medium) on internal systems (approximately 22,000 hosts)."[98] Of the known vulnerabilities at the time, "approximately **75%** of the external, and **93%** of the internal, [sic] vulnerabilities are over 90 days old."[99]

The following graphic depicts the more than 1,000 critical/high/medium risk vulnerabilities, by age, which existed on Equifax's external-facing systems at the time of the audit report.[100]

[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] EFXCONG-PSI000032256.
[98] *Id.*
[99] *Id.*
[100] EFXCONG-PSI000032258.



These systems were "accessible from outside the Equifax network and could be vulnerable to exploitation by hackers."[101] More than 65 percent of these vulnerabilities were more than 90 days old.[102]

3. Key Audit Findings Demonstrate Equifax's Ineffective Patch and Configuration Management

The audit report also identified numerous findings and recommendations related to Equifax's configuration and patch management procedures, five of which are highlighted below. First, the audit found that Equifax was not remediating vulnerabilities in a timely fashion.[103] Second, the audit identified the security risks associated with Equifax's lack of a comprehensive IT asset inventory.[104] Third, the audit found that Equifax's IT department was not proactively applying patches throughout its network.[105] Fourth, the audit highlighted Equifax's failure to verify the successful implementation of patches.[106] Finally, the audit found that Equifax's

[101] EFXCONG-PSI000032257.
[102] EFXCONG-PSI000032258.
[103] *See infra* Part III.A.3.a.
[104] *See infra* Part III.A.3.b.
[105] *See infra* Part III.A.3.c.
[106] *See infra* Part III.A.3.d.

2015 policy did not adequately consider the criticality of an asset when determining a patching schedule.[107] Each finding is discussed in further detail below.

a. Equifax Did Not Follow Its Own Schedule for Remediating Vulnerabilities

The audit revealed that Equifax did not fix vulnerabilities in a timely manner.[108] For example, there were "over 8500 [sic] medium, high or critical vulnerabilities existing with a large percentage of those being over 90 days outstanding."[109] According to the report, the lack of prompt remediation of vulnerabilities "creates a security exposure and could allow Equifax systems and data to be compromised."[110] In interviews with the Subcommittee, the Senior Vice President of Product Security and the former CSO expressed a lack of concern over the number of outstanding vulnerabilities highlighted in the audit, instead indicating that the volume naturally fluctuated.[111] The former CSO emphasized that the nature of specific vulnerabilities was a more important factor and that the total number included a wide range of types of vulnerabilities.[112] Equifax's Senior Vice President of Product Security stated that any vulnerability was troubling to him, but added that seeing a particular number of vulnerabilities would not necessarily surprise him without knowing more about the nature of those vulnerabilities.[113]

The report recommended addressing slow remediation efforts by implementing automated tools, and management responded by committing to leverage or implement those tools by December 31, 2016.[114] The recommended automated tools were not in place company-wide by the proposed deadline.[115] While Equifax was making progress, they still had not fully implemented the recommended automated tool by the time the public learned of the Apache Struts vulnerability in March 2017.[116] In fact, efforts are still ongoing at the company to further enhance the process. Equifax has appointed "patch champions" to oversee and confirm patch installation throughout the network.[117]

---

[107] *See infra* Part III.A.3.e.
[108] EFXCONG-PSI000032259.
[109] *Id.*
[110] *Id.*
[111] Interview with the Senior Vice President of Product Security, Equifax (Aug. 30, 2018) [hereinafter Senior Vice President of Product Security Interview Aug. 30, 2018)]; Former CSO Interview (Oct. 4, 2018).
[112] Former CSO Interview (Oct. 4, 2018).
[113] Senior Vice President of Product Security Interview (Aug. 30, 2018).
[114] EFXCONG-PSI000032259.
[115] Interview with Director, Security-Threats-Vulnerabilities, Equifax (Aug. 19, 2018) [hereinafter Former GTVM Director Interview (Aug. 19, 2018)]; Interview with the former Chief Information Officer, Equifax (Oct. 31, 2018) [hereinafter Former CIO Interview (Oct. 31, 2018)].
[116] Former GTVM Director Interview (Aug. 19, 2018).
[117] Briefing with Equifax (Mar. 27, 2018).

b. Equifax Lacked a Comprehensive IT Asset Inventory

The second audit finding revealed that, as of 2015, Equifax did not have a complete IT asset inventory or accurate network documentation.[118] According to the report, the risk of not having this inventory "makes it difficult to ensure systems are patched in a timely manner and are being regularly scanned for security vulnerabilities."[119] Having an asset inventory is "paramount" from a security standpoint, because an organization can only defend the assets it has identified.[120] Equifax's former Vice President of its Cyber Threat Center ("CTC") told the Subcommittee that without an inventory, an organization would be unaware of the need to scan particular assets for vulnerabilities. She added that having an asset inventory is a best practice, but Equifax may have experienced a lag time in updating any asset inventory because the company continually grows by buying other entities and integrating their systems into Equifax's.[121]

In response to this finding, the audit report recommended that management "ensure a current and accurate accounting of all IT assets is available at all times."[122] Management proposed a multistep action plan to respond to this finding with an estimated remediation date of June 30, 2017.[123]

At the time of the breach, in late July 2017, there was no complete inventory in place.[124] Equifax's Senior Vice President of Product Security stated that the company was making a concerted effort, following the breach, to improve its inventory.[125] Efforts to complete a physical and virtual asset inventory are still ongoing.[126]

c. Equifax Had a Reactive Patching Process

The audit's third finding showed that "most Equifax systems are not patched in a timely manner."[127] This same finding also concluded that the company was

---

[118] EFXCONG-PSI000032260.
[119] *Id.*
[120] Interview with Manager, Countermeasures, Equifax (Sept. 12, 2018) [hereinafter Former Countermeasures Manager Interview (Sept. 12, 2018)].
[121] Interview with Manager, Cyber Threat Center, Equifax (Aug. 27, 2018) [hereinafter Former VP of the CTC Interview (Aug. 27, 2018)].
[122] EFXCONG-PSI000032260.
[123] *Id.*
[124] Former GTVM Director Interview (Aug. 19, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former CSO Interview (Oct. 4, 2018).
[125] Senior Vice President of Product Security Interview (Aug. 30, 2018).
[126] Briefing with Equifax (Sept. 24, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018).
[127] EFXCONG-PSI000032260.

using threat and vulnerability information to "reactively patch their systems instead of proactively applying patches."[128] According to the report, this reactive patching practice caused Equifax systems to remain susceptible until the GTVM team notified the IT department of specific vulnerabilities. The audit recommended that management document and implement a proactive patching process; management responded by providing an action plan and an estimated remediation date of December 31, 2016. Specific business units within the company had implemented a proactive patching process, but it was not consistent company-wide at the time of the breach.[129]

d. Equifax Used an "Honor System" for Patching

The fourth finding revealed that Equifax was using an "honor system" to ensure patches were installed successfully. [130] According to the audit, the following five Equifax groups and teams were responsible for configuration and patch management: "1) Security, 2) Application Services, 3) Global Corporate Platforms, 4) Risk Programs, and 5) Back Office Support (desktop support)."[131] At the time of the audit, the vulnerability management process involved scanning for, identifying, and notifying the relevant parties of vulnerabilities.[132] Upon completion of the scans, Equifax would only apply patches when scans confirmed the existence of a vulnerability.[133] Consistent with the "honor system" description, the Subcommittee found no evidence that Equifax tracked the completion or success of patch implementation. If the scan detected no vulnerabilities, Equifax would take no further action.[134]

According to Equifax's former Countermeasures Manager, this is not an advisable approach to patching.[135] Instead, he recommended implementing a system that verified scan results before deciding to take no further action.[136] He also told Subcommittee staff that when he heard the term "honor system," he thought it meant that each asset user and operator would be responsible for verifying patch installation, but he acknowledged it was not a term he heard at Equifax before.[137] The former CIO indicated that he did not know why Equifax was using an honor system to ensure proper patching.[138] He further stated that the

---

[128] *Id.*
[129] Former GTVM Director Interview (Aug. 19, 2018).
[130] EFXCONG-PSI000032261.
[131] EFXCONG-PSI000032257.
[132] Former GTVM Director Interview (Aug. 19, 2018).
[133] Briefing with Equifax (Mar. 27, 2018).
[134] *Id.*; Former Countermeasures Manager Interview (Sept. 12, 2018).
[135] Former Countermeasures Manager Interview (Sept. 12, 2018).
[136] *Id.*
[137] *Id.*
[138] Former CIO Interview (Oct. 31, 2018).

security team, not IT, was responsible for verifying patch installation, but he did not know whether they were actively tracking that information.[139]

The management response to the "honor system" finding was to "build and provide a centralized tracking capability."[140] At the time of the breach, Equifax had a vulnerability tracking system in place, but that system had no processes in place to make managers aware of vulnerabilities that were not addressed in a timely manner.[141] Since the breach, the IT department now installs patches proactively and "patch champions" have responsibility for ensuring their successful installation, regardless of the results of a network scan.[142]

e. Equifax Did Not Consider the Criticality of IT Assets When Patching

The audit's final finding showed that Equifax's 2015 patch management policy did not consider the criticality of an IT asset in determining when to require a patch for the system.[143] According to the report, without an asset criticality assessment, the policy "would allow a high risk patch [to remain] on a critical server for 30 days before it is required to be patched."[144] This created a scenario where critical assets might remain vulnerable while the company prioritized remediating less critical assets.[145]

The recommendation in response to this finding was to enhance the patch management policy to include "more stringent patching requirements for high risk systems."[146] The estimated remediation date for this issue was December 31, 2015.[147] The former CIO told the Subcommittee that he was unaware of any changes to the policy in response to this recommendation, although he added that the company could have addressed the issue through procedural changes.[148] The former Vice President of the CTC also told Subcommittee staff that she still observed a lack of criticality assessment upon her arrival at Equifax in September 2016.[149]

---

[139] *Id.*
[140] EFXCONG-PSI000032261.
[141] *Id.*
[142] Briefing with Equifax (Mar. 27, 2018); Briefing with Equifax (Sept. 24, 2018).
[143] EFXCONG-PSI000032263.
[144] *Id.*
[145] Former VP of the CTC Interview (Aug. 27, 2018).
[146] EFXCONG-PSI000032263.
[147] *Id.*
[148] Former CIO Interview (Oct. 31, 2018).
[149] Former VP of the CTC (Aug. 27, 2018).

4. Equifax Conducted No Follow-Up Audits After the 2015 Audit

Following the breach, which occurred nearly two years after the patch management audit, the Senior Vice President of Equifax's Internal Audit group informed the former CSO that, as of August 2017, the audit team had "not done a formal follow-up" to the 2015 report.[150] In an interview with Subcommittee staff, the former CSO indicated there was direct follow-up to the audit.[151] When pressed to substantiate this audit follow-up, Equifax pointed to several documents such as one from May 2016 that reflected draft language to include in the "ERM [Enterprise Risk Management] deck related to Patch Management activities."[152] Equifax officials claim the company took steps to address both externally and internally facing vulnerabilities identified in the audit report.[153] Equifax also confirmed that Internal Audit had not conducted a formal re-audit of the topics in the patch management audit.[154]

In addition, an August 2017 document highlighted IT and security updates that were underway nearly two years after the audit and one month after Equifax discovered the breach.[155] When asked about this document, the former CIO informed Subcommittee staff that it was a presentation for a regular monthly meeting he had with the former CSO to discuss "key initiatives and capital investments" being addressed by the IT and security teams.[156] Yet this document makes no specific reference to any ongoing efforts that were directly in response to the findings from the 2015 patch management audit. Another document, also from August 2017, stated that the "global patching process continues [sic] at risk as we cannot adequately address the patching issues without moving the legacy applications to current versions of the systems software as it would lead to significant operational risk."[157] At least four current and former Equifax employees the Subcommittee interviewed did not recall another patch management audit during their tenure with the company.[158] Equifax officials have informed Subcommittee staff that its Internal Audit function now evaluates patch management as part of its regularly scheduled review.[159]

---

[150] EFXCONG-PSI000032255.
[151] Former CSO Interview (Oct. 4, 2018).
[152] Letter from Equifax to the Subcommittee (Oct. 16, 2018); EFXCONG-PSI000039073.
[153] Letter from Equifax to the Subcommittee (Oct. 16, 2018); EFXCONG-PSI000039242–73; EFXCONG-PSI000035979–83.
[154] Letter from Counsel for Equifax to Subcommittee staff (Oct. 16, 2018).
[155] EFXCONG-PSI000039242–73.
[156] Former CIO Interview (Oct. 31, 2018).
[157] EFXCONG-PSI000035979–83.
[158] Former Countermeasures Manager Interview (Sept. 12, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former CSO Interview (Oct. 4, 2018); Former CIO Interview (Oct. 31, 2018).
[159] Briefing with Equifax (Sept. 26, 2018).

B. Patching Issues Remained Leading up to the Breach in 2017

In early 2017, sixteen months after the release of the patch management audit report, members of the IT department and security team were still working to improve the patch management process. In addition, on February 2, 2017, an Information Security Compliance Analyst in Canada identified security issues and suggested a project specifically to improve patch management, which she referred to as the "Green Belt project."[160] The goal of this proposed Green Belt project would have been to address eight issues, three of which are relevant to the Subcommittee's findings and discussed below. Although Equifax never formally adopted the Green Belt project, these suggestions highlight the numerous outstanding patching issues at Equifax prior to the 2017 breach.[161]

1. Equifax's Scan Process Was Global; Patch Management Was Regional

The proposed Green Belt project noted that Equifax's system for vulnerability scanning was a global process that was disconnected from the company's regional patch management process.[162] Equifax's former Director of the GTVM team told Subcommittee staff that in some cases, patching was regional, and some cases it was global.[163] He indicated that "IT leadership" – specifically, "[the former CIO] and his team" – put that system in place.[164] When the Subcommittee asked about this project, the former CIO indicated he was not familiar with it, but he confirmed that the IT team's patching process was regional because the infrastructure was different across global offices.[165] He further noted that the difference between the global nature of the system's vulnerability scanning and the regional nature of the patch management process was not "that important."[166]

The recommendation in response to this issue was to connect the scanning and patching processes to improve overall system performance.[167] Five of the current or former Equifax employees the Subcommittee interviewed were not aware whether action was taken to connect the scanning and patching processes.[168] Equifax told the Subcommittee there was no Green Belt project developed as a

---

[160] EFXCONG-PSI000028724–26. Through Counsel, Equifax explained that "green belt" was a reference to the Six Sigma project improvement terminology used generically in the business community to describe a type of project. Letter from Counsel for Equifax (Feb. 20, 2019).
[161] Email from Counsel for Equifax to Subcommittee staff (Feb. 1, 2019).
[162] EFXCONG-PSI000028724.
[163] Former GTVM Director Interview (Aug. 19, 2018).
[164] *Id.*
[165] Former CIO Interview (Oct. 31, 2018).
[166] *Id.*
[167] EFXCONG-PSI000028724.
[168] Former GTVM Director Interview (Aug. 19, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former CSO Interview (Oct. 4, 2018); Former CIO Interview (Oct. 31, 2018).

result of this proposal.[169] Equifax instead stated that members of the global IT department and global security department at Equifax were contemporaneously involved in efforts to enhance the patch management process, including some of the topics discussed in the proposed Green Belt project.[170]

2. It Was Unclear Whether IT Was Following Patch Management and Vulnerability Management Procedures

The second area targeted for improvement in the proposed Green Belt project involved ensuring that Equifax employees were following patch management and vulnerability management policies company-wide.[171] To improve patch management, the Information Security Compliance Analyst recommended identifying: "the mandatory processes as per the approved (policy and standard) for all [business units] to implement and govern. Confirm the intent and implementation of these documents at the regional level, such as training, exception, internal auditing, etc."[172]

Upon initiation of this effort, there was a repeatable process for scans, but not for patch management.[173] According to the former GTVM Director, these processes were not repeatable at that point in time, due to a lack of technology and personnel resources to implement the necessary automation process.[174] When asked about this assertion, the former CIO told Subcommittee staff he was not aware of insufficient personnel resources to handle patch management issues.[175]

3. Equifax Needed a New Scanning Tool

The proposed Green Belt project's third targeted area for improvement was the implementation of a new scanning tool.[176] According to the Security analyst, the new scanning tool "would improve the clarity of output of scan reports and would likely grow the number of vulnerabilities that leads us to a new risks approach."[177] The Security analyst believed that the scanning tool

---

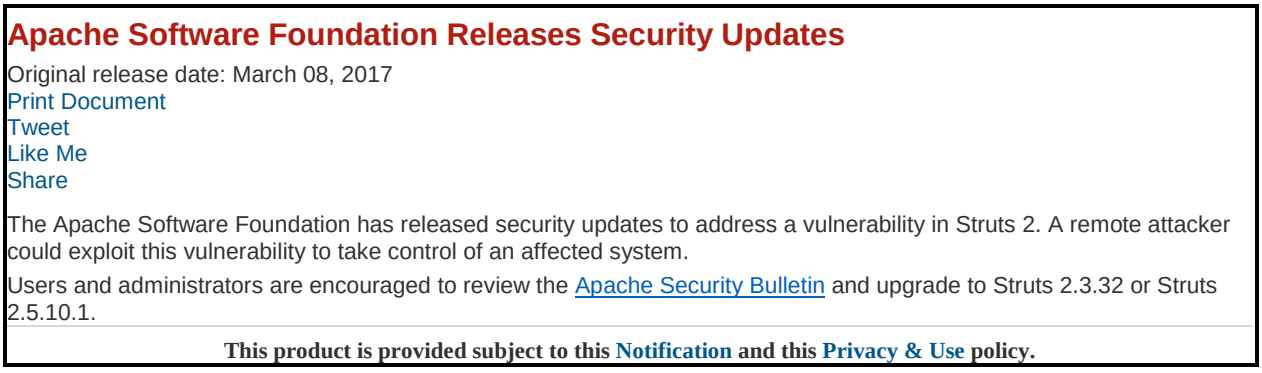
[169] Email from Counsel for Equifax to Subcommittee staff (Feb. 1, 2019).
[170] *Id.*
[171] EFXCONG-PSI000028724–26.
[172] *Id.*
[173] Former GTVM Director Interview (Aug. 19, 2018).
[174] *Id.*
[175] Former CIO Interview (Oct. 31, 2018). In a subsequent email, Counsel for the former CIO noted "significant additional resources devoted and people hired to accelerate patching efforts," including automation, internal tracking, and the funding or implementation of various initiatives. Email from Counsel for the former CIO to Subcommittee staff (Feb. 20, 2019).
[176] EFXCONG-PSI000028724–26.
[177] *Id.*

would create "less base patching issues from the historic process – ie. [sic] Clean up the backlog."[178] When asked about this backlog, the former GTVM Director told the Subcommittee the patching backlog was "a couple years' long."[179]

Equifax believed the new scanning tool also had more capabilities than Equifax's initial scanner and would enable greater visibility into the network to identify more vulnerabilities.[180] Equifax approved the implementation of the new scanner in 2016, with accompanying funding in 2017.[181] Equifax was not using the scanner at the time of the Apache Struts vulnerability announcement, but it was operational for external systems in approximately June or July 2017.[182]

III. EQUIFAX'S RESPONSE TO THE VULNERABILITY THAT FACILITATED THE BREACH WAS INADEQUATE AND HAMPERED BY ITS NEGLECT OF CYBERSECURITY

On March 8, 2017, US-CERT sent out an alert, CVE-2017-5638, announcing a vulnerability in certain versions of Apache Struts, as shown in the image below.[183]



Apache Software Foundation Releases Security Updates

Original release date: March 08, 2017
Print Document
Tweet
Like Me
Share

The Apache Software Foundation has released security updates to address a vulnerability in Struts 2. A remote attacker could exploit this vulnerability to take control of an affected system.

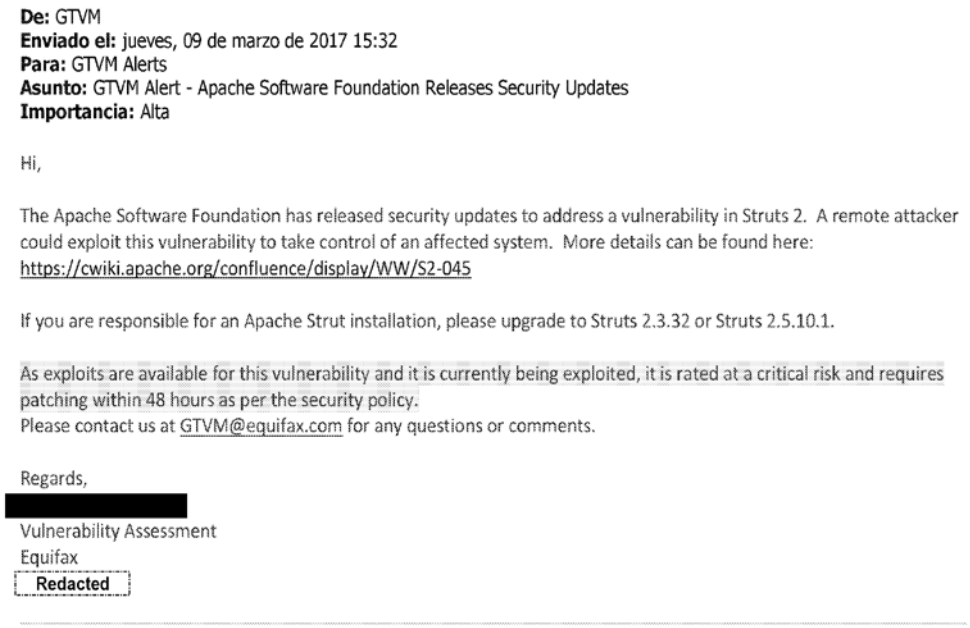
Users and administrators are encouraged to review the Apache Security Bulletin and upgrade to Struts 2.3.32 or Struts 2.5.10.1.

This product is provided subject to this Notification and this Privacy & Use policy.

Equifax's GTVM team received CVE-2017-5638 on March 8 from US-CERT.[184] The GTVM team circulated the notice internally through an alert sent to the GTVM Alerts distribution list on March 9, 2017.[185] At the time, that

[178] *Id.*
[179] Former GTVM Director Interview (Aug. 19, 2018).
[180] EFXCONG-PSI000028725.
[181] Former GTVM Director Interview (Aug. 19, 2018).
[182] *Id.*
[183] Apache Software Foundation Releases Security Updates, US-CERT (Mar. 8, 2017), https://www.us-cert.gov/ncas/current-activity/2017/03/08/Apache-Software-Foundation-Releases-Security-Updates.
[184] EFXCONG-PSI000003371–72.
[185] EFXCONG-PSI000036370–73.

distribution list consisted of more than 400 Equifax employees.[186] The GTVM alert restated verbatim the US-CERT language, as shown in the image below.[187]



De: GTVM
Enviado el: jueves, 09 de marzo de 2017 15:32
Para: GTVM Alerts
Asunto: GTVM Alert - Apache Software Foundation Releases Security Updates
Importancia: Alta

Hi,

The Apache Software Foundation has released security updates to address a vulnerability in Struts 2. A remote attacker could exploit this vulnerability to take control of an affected system. More details can be found here:
https://cwiki.apache.org/confluence/display/WW/S2-045

If you are responsible for an Apache Strut installation, please upgrade to Struts 2.3.32 or Struts 2.5.10.1.

As exploits are available for this vulnerability and it is currently being exploited, it is rated at a critical risk and requires patching within 48 hours as per the security policy.
Please contact us at GTVM@equifax.com for any questions or comments.

Regards,
[redacted]
Vulnerability Assessment
Equifax
Redacted

The tools to exploit the March 2017 Apache Struts vulnerability were publicly available and easy to use.[188] Yet, in the weeks and months that followed US-CERT's public notice of the vulnerability, Equifax employees were unable to respond adequately due to a failure to implement basic cybersecurity standards, which prevented Equifax from complying with its own internal policies and procedures. Equifax lacked a comprehensive IT inventory, so it was unable to locate the vulnerable Apache Struts application on its network, which rendered its policy to patch critical vulnerabilities within 48 hours useless.[189] Company officials discussed the Apache Struts vulnerability at the monthly meetings called to highlight these types of vulnerabilities in March and April but did not discuss the vulnerability in subsequent meetings.[190] The software developer who was aware that Equifax ran vulnerable versions of Apache Struts never received the alert because the distribution list used to disseminate it did not include all application owners.[191] Equifax scanned its network repeatedly but those scans never identified vulnerable versions of Apache Struts.[192] Expired SSL certificates delayed Equifax's ability to detect the intrusion for months.[193]

---

[186] Former GTVM Director Interview (Aug. 19, 2018).
[187] EFXCONG-PSI000036370–73.
[188] *See infra* Part IV.A.
[189] *See infra* Part IV.B.
[190] *See infra* Part IV.C.
[191] *See infra* Part IV.D.
[192] *See infra* Part IV.E.
[193] *See infra* Part IV.F.

In the weeks following US-CERT's public notification, hackers successfully breached a web application running a vulnerable version of Apache Struts located on the Equifax network. When they did, they were able to access multiple data repositories due to Equifax's decision not to implement certain cybersecurity protocols recommended in the NIST cybersecurity framework.[194] Specifically, the combination of expired SSL certificates, unencrypted usernames and passwords, and a lack of network segmentation – all discussed in more detail below – compounded the effect of the breach. After learning of the breach and the access the hackers gained to multiple company systems, Equifax waited six weeks to notify the public.[195] Therefore, since hackers had access to the data as early as May 13, 2017, the public was unaware that its data was compromised for over sixteen weeks. Several current and former Equifax employees still believe Equifax's response to the vulnerability was appropriate.[196]

A. The Tools Necessary to Exploit the March 2017 Apache Struts Vulnerability Were Publicly Available and Easy to Use

The Deputy Director of DHS's NCCIC, Chris Butera, discussed the March 2017 Apache Struts vulnerability in a briefing to the Subcommittee.[197] Deputy Director Butera indicated that Apache Struts is a very common open source web application used on many U.S.-based networks and can be difficult to patch because of the manual nature of the patching process.[198] A patch is a "'repair job' for a piece of programming; it is also known as a 'fix.'"[199] Vendors typically create and distribute patches as a replacement for or an insertion in compiled code.[200] DHS learned of the Apache Struts vulnerability in March 2017 through its vulnerability analysis work.[201] Deputy Director Butera noted that a CVSS score of 10 – the highest criticality score a vulnerability can receive – was assigned by NIST to the Apache Struts vulnerability because of the ease of exploitation, remote code execution ability, and the ability to gain unauthorized privileged access.[202]

In a separate briefing to the Subcommittee, Mandiant, a private cybersecurity firm that provides post-breach response and forensic examination

---

[194] *See infra* Part IV.G.
[195] *See infra* Part IV.H.
[196] *See infra* Part IV.I.
[197] Briefing with the National Cybersecurity & Communications Integration Center, U.S. DEP'T OF HOMELAND SECURITY (Jan. 18, 2018).
[198] *Id.*
[199] NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, *Guidelines on Securing Public Web Servers* B-1 (2007).
[200] *Id.*
[201] Briefing with the National Cybersecurity & Communications Integration Center, U.S. DEP'T OF HOMELAND SECURITY (Jan. 18, 2018).
[202] *Id.*

services, also discussed the Apache Struts vulnerability.[203] Mandiant explained that the necessary code and accompanying instructions to exploit the Apache Struts vulnerability became publicly available four days before a patch became available on the website GitHub.com, a development platform used by millions of businesses and organizations to develop and build software.[204] The exploit code, which was published by a researcher, had reliability approaching 100 percent in Mandiant's testing environment, which involves default out-of-box installations of the vulnerable application, according to Mandiant officials, which is notable because exploit codes do not always work.[205] Mandiant stressed the ease of exploiting this vulnerability by noting: "Even a trivial modification of the information and instructions published on GitHub could result in a functional exploit. Individuals with even low-level knowledge of computers could conduct some research, make use of the vulnerability, and perform the attack themselves."[206]

Mandiant representatives also noted that the patch for this vulnerability was easy to deploy if the default installation of Struts was utilized.[207] However, they indicated that patching could be difficult for companies that lacked an asset inventory or otherwise did not know what parts of their systems were using Apache Struts.[208] According to Mandiant, a company would ideally have an up-to-date asset inventory and could identify the location of a vulnerability on its network, determine whether a patch is needed, and apply the patch within 72 hours.[209] If a company lacks an accurate inventory, it will need to take additional time to perform scans of its network and validate the presence of vulnerable systems.[210] When applying a patch, companies will also need to test it before installation to make sure it solves the problem without any unintended consequences.[211]

Mandiant also stated that companies face difficulties in patching critical vulnerabilities because companies receive notice of thousands of vulnerabilities each month.[212] In 2017, for example, the National Vulnerability Database scored 2,165 vulnerabilities as critical (a score of 9 or 10), which was approximately 15 percent of all vulnerabilities.[213] This equates to about five critical vulnerabilities per day.[214] According to Mandiant, deciding which critical vulnerabilities to

---

[203] During this briefing, Mandiant did not reveal the identity of any of its clients nor discuss any specific cases with the Subcommittee. Briefing with Mandiant (Mar. 1, 2018).
[204] Representatives from Mandiant also stated that the exploit had "commodity-like availability on the black market." Briefing with Mandiant (Mar. 1, 2018).
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.*
[213] Email from National Institute of Standards and Technology to Subcommittee staff (Feb. 15, 2019).
[214] Briefing with Mandiant (Mar. 1, 2018).

prioritize is a key challenge for cybersecurity professionals: "If everything is critical, then nothing is critical."[215]

B. Equifax Did Not Follow Its Patch Management Policy When Responding to the Apache Struts Vulnerability

At the time of US-CERT's Apache Struts notification, the former CSO oversaw the company's security group, which consisted of approximately 180-190 people working in various subgroups.[216] According to the former CSO, "at a general level, security would set policy and standards that IT had to follow."[217] During this same time period, the former CIO oversaw the company's IT department.[218] Equifax's patch management policy required the IT department to patch critical vulnerabilities within 48 hours.[219] Despite categorizing the Apache Struts vulnerability as critical in March 2017, Equifax did not patch the Apache Struts vulnerability until August 2017 because it lacked a comprehensive IT inventory and was unable to locate the vulnerability on its network.[220]

1. Equifax's Patch Management Policy Required the IT Department to Patch Critical Vulnerabilities Within 48 Hours

Prior to 2015, Equifax had no formal standalone guidance governing patch management.[221] Equifax created its original patch management policy in April 2015 at the direction of the former CSO, who expressed concern to the then-CIO about the lack of a formal, written policy.[222] The version of the policy in effect in March 2017 identified several different types of patches, including functionality, performance, and security.[223] Security patches have four characterizations: critical; high risk; medium risk; and low risk.[224] The policy established the following patch installation schedule for each category of security patches:[225]

Patch Category	Patch Deployment Times
Critical Patch	"[T]o be installed within 48 hours from time of release or in timeframe agreed with Security."

[215] *Id.*
[216] Former CSO Interview (Oct. 4, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018).
[217] Former CSO Interview (Oct. 4, 2018).
[218] Former CIO Interview (Oct. 31, 2018).
[219] *See infra* Part IV.B.1.
[220] *See infra* Part IV.B.2.
[221] Former CSO Interview (Oct. 4, 2018).
[222] *Id.*
[223] EFXCONG-PSI000000200.
[224] *Id.*
[225] *Id.*

High Risk Patch	"[T]o be installed within 30 days from time of release or in timeframe agreed with Security."
Medium Risk Patch	"[T]o be installed within 90 days from time of release or in timeframe agreed with Security."
Low Risk Patch	"[T]o be installed within the normal patching rotation, but within at least a year from time of release or in timeframe agreed with Security."

While the security department is responsible for identifying and monitoring cyber vulnerabilities, the IT department, which has over 8,000 employees, is responsible for applying patches and typically did so during scheduled maintenance windows.[226] Equifax refers to this as the "normal patching rotation."[227] Vulnerabilities deemed critical, however, fell outside of this normal patching rotation.[228] IT employees responsible for applying patches would receive information from the security team on the criticality of each vulnerability and whether it should be patched.[229] The security team was responsible for validating the completion of the patch process by scanning the environment to determine if a patch was successfully applied.[230] If a scan did not reveal a vulnerability, the security team would assume that the patch was successfully applied or that the vulnerability did not exist.[231]

The patching process itself is complex and involves several different groups and teams within Equifax.[232] Individuals responsible for managing company business units, IT systems, and applications within systems each play a role in the installation of a patch.[233] Managers of company business units are responsible for ensuring that an IT asset, such as an application, works as intended.[234] Equifax assigns system owners to each IT asset and they are responsible for installing patches on their respective systems.[235] Application owners are responsible for ensuring that system owners properly install patches on a system and that the patch does not negatively impact applications.[236] Equifax maintained a centralized list of system and application owners prior to the breach, but the list was ambiguous and not properly maintained.[237] All of the IT teams ultimately reported

[226] Senior Vice President of Product Security Interview (Aug. 30, 2018).
[227] EFXCONG-PSI000000200.
[228] Former CSO Interview (Oct. 4, 2018).
[229] Briefing with Equifax (Mar. 27, 2018).
[230] *Id.*
[231] *Id.*
[232] Briefing with Equifax (Sept. 24, 2018).
[233] *Id.*
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.*

to the former CIO.[238] The former CIO described patching as a "lower level responsibility that was six levels down" from him.[239] He also stated that he was not responsible for patching and that it was not something he spent time on.[240]

2. Equifax Did Not Patch the Apache Struts Vulnerability Until August 2017

Equifax's patch management policy required the deployment of a critical patch within 48 hours from the time of release.[241] While Equifax was aware of the criticality of the Apache Struts vulnerability identified in CVE-2017-5638, no Equifax employee began patching the vulnerability until after the July breach because Equifax had an incomplete IT inventory, which rendered the company unable to identify the vulnerability in its environment.[242] The patch for the Apache Struts vulnerability was applied the week after August 2, 2017, nearly five months after the public announcement of the vulnerability.[243] Equifax acknowledged to the Subcommittee that "the vulnerability should have been patched within 48 hours."[244] Although many of Equifax's cybersecurity policies and procedures reference consequences for non-compliance, the Subcommittee was unable to identify any examples throughout its investigation of any actions taken against company employees who failed to comply.[245]

C. Equifax Held Monthly Meetings to Discuss Threats and Vulnerabilities, but Follow-Up Was Limited and Key Senior Managers Did Not Attend

Monthly GTVM meetings discussed threats and vulnerabilities.[246] Monthly GTVM meetings consist primarily of IT and security team members discussing the corresponding slide deck made available prior to the meeting.[247] The GTVM team also fielded questions at the meeting about items in the slide deck, which included security news, end of support notices, and third-party patches.[248] Vulnerabilities

---

[238] Former CIO Interview (Oct. 31, 2018).
[239] *Id.*
[240] *Id.*
[241] EFXCONG-PSI000000200.
[242] Briefing with Equifax (Mar. 27, 2018).
[243] *Id.*
[244] *Id.*
[245] Former GTVM Director Interview (Aug. 19, 2018); Former VP of the CTC Interview (Aug. 27, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018); Former CSO Interview (Oct. 4, 2018); Former CIO Interview (Oct. 31, 2018).
[246] The meetings are global and held telephonically. Former VP of the CTC Interview (Aug. 27, 2018).
[247] Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019).
[248] Former Countermeasures Manager Interview (Sept. 12, 2018). *See also* EFXCONG-PSI000034542.

listed in a given month's slide deck do not carry over to the next month's slide deck even if they have not been remediated.[249] Equifax did not require any employee to attend this monthly meeting, although there was an "expectation" that certain individuals would.[250] Prior to the breach, Equifax did not consistently track who attended.[251] It was also unclear whether senior managers from Equifax's security teams attended the meetings. Senior managers interviewed by the Subcommittee provided varying responses.[252] For example, one senior manager could not recall if they listened to the calls.[253] Another senior manager sent someone in their stead.[254] Yet another stated they participated when they were able and received a readout when they were unable to participate.[255]

1. Equifax Highlighted the Apache Struts Vulnerability in Its March GTVM Meeting

Separate from the monthly slide decks identifying many of the latest vulnerabilities and security updates, the GTVM team occasionally sent alerts that it described as "out-of-band."[256] The goal of these out-of-band alerts was to highlight critical issues that were so important that discussion should not wait until the following monthly meeting.[257] The March 9 Apache Struts alert about CVE-2017-5638 was an out-of-band alert.[258] GTVM sent these alerts an average of once every one to two months and "were typically pretty good" about patching them within 48 hours.[259]

The GTVM team also discussed the Apache Struts alert at the monthly meeting on March 16, 2017.[260] Attendees received a briefing on the vulnerability and, according to Equifax's Deputy Chief Information Security Officer ("Deputy CISO"), sought to make sure appropriate response efforts were progressing.[261] The March 2017 GTVM slide deck included CVE-2017-5638 on the list of third-party patches, and stated that the vulnerability was currently being exploited, explained it could allow an attacker to take control of an affected system, and listed the

---

[249] *Id.*
[250] Briefing with Equifax (Sept. 24, 2018).
[251] *Id.*
[252] Former GTVM Director Interview (Aug. 19, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018); Former CSO Interview (Oct. 4, 2018); Former CIO Interview (Oct. 31, 2018).
[253] Former GTVM Director Interview (Aug. 19, 2018).
[254] Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019).
[255] Former VP of the CTC Interview (Aug. 27, 2018).
[256] *Id.*
[257] *Id.*
[258] Briefing with Equifax (Sept. 24, 2018).
[259] Former GTVM Director Interview (Aug. 19, 2018).
[260] Briefing with Equifax (Sept. 24, 2018).
[261] *Id.*

versions of Struts that were affected.[262] It also contained instructions to upgrade certain versions of Struts and included the link to the Apache Security Bulletin.[263] Since Equifax did not always track which employees dialed into GTVM meetings, Equifax did not have a consistent way of knowing which employees attended the meetings.[264] The Apache Struts vulnerability is referenced in the April 2017 GTVM slide deck, but unlike the March slide deck, the vulnerability did not appear on the list of third-party patches or contain instructions to upgrade to a newer version.[265] The July GTVM slide deck produced to the Subcommittee did not reference the Apache Struts vulnerability.[266]

2. Prior to the Breach, Senior Managers from Equifax Security Teams Did Not Regularly Participate in These Monthly Meetings

The Subcommittee interviewed several senior members of Equifax's cybersecurity team who were in place from March to September 2017. This included the CSO, the Senior Vice President of Product Security, the Vice President of the CTC, the Director of GTVM, and the Manager of Countermeasures. None of these individuals could recall attending the GTVM monthly meeting held on March 16, 2017, where GTVM discussed the critical Apache vulnerability.[267]

These individuals also indicated that they, along with members of the Senior Leadership Team, did not regularly attend the monthly GTVM meetings.[268] The former GTVM Director and the former Vice President of the CTC indicated that they would attend when able, but otherwise would receive read-outs from subordinates or colleagues who attended.[269] The Senior Vice President of Product Security and the former Countermeasures Manager indicated that they did not

---

[262] EFXCONG-PSI000034551.
[263] *Id.*
[264] Briefing with Equifax (Sept. 24, 2018).
[265] EFXCONG-PSI00034494–530. The April 2017 slide deck did contain a slide titled "Threat Watch," on which "Apache Struts Recon" appears under the category "[Equifax] Threat Activity Highlights." The same GTVM slide deck for April 2017 included a slide titled "Cyber Intelligence Highlights for March," which includes "Apache Struts Vulnerability attempts" among a list of items. *Id.*
[266] *See* EFXCONG-PSI000002779–812.
[267] Former GTVM Director Interview (Aug. 19, 2018); Former VP of the CTC Interview (Aug. 27, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018); Former CSO Interview (Oct. 4, 2018).
[268] *Id.* The Subcommittee did not receive copies of calendars for any Equifax employees.
[269] Former GTVM Director Interview (Aug. 19, 2018); Former VP of the CTC Interview (Aug. 27, 2018). Counsel for the former CSO indicated she received weekly vulnerability assessment reports and frequently received daily updates from the cybersecurity team; she also met regularly with senior leadership to review security issues. Email from Counsel for the former CSO to Subcommittee staff (Feb. 20, 2019). Counsel for the former VP of the CTC indicated that she "participated as she was able." Email from Counsel for former VP of the CTC to Subcommittee staff (Feb. 20, 2019).

request readouts but would wait to see if anyone reached out to them with a specific question or concern.[270] The former CIO indicated that he "never" learned about vulnerabilities announced by US-CERT, including the March 8 alert concerning the Apache Struts vulnerability.[271]

The head of the Countermeasures team, who was responsible for ensuring that appropriate countermeasures were in place to block attempts to exploit identified vulnerabilities, told the Subcommittee that the items listed in the monthly GTVM slide deck served as an informational report for his team more than as a "to-do list."[272]

D. The Equifax Employee Who Was Aware of Equifax's Use of Apache Struts Software Was Not on the Relevant Email Distribution List

Only one of the more than 400 individuals on the GTVM distribution list responded to the March 9 alert regarding CVE-2017-5638.[273] On March 14, 2017, five days after the GTVM team issued the alert, an Equifax employee in Spain responded, noting that his office was using two different versions of Struts and that neither was among the versions listed as vulnerable in the alert.[274] He requested confirmation that his conclusion was accurate and noted that the business impact could be quite heavy if he was incorrect.[275] A GTVM team member responded the same day confirming that both versions were not vulnerable to the exploit US-CERT had warned about; however, he also noted that both versions in use in Spain were old and no longer supported by Apache. Both had vulnerabilities that were several years old and had not been fixed.[276]

The lead developer who was aware that the company was using Apache Struts in the online dispute portal was not included on the GTVM distribution list.[277] The senior manager that the developer ultimately reported to did receive the alert but did not forward it to the developer or anyone else on the developer's team.[278] As a result, this developer did not receive the GTVM alert about the Apache Struts vulnerability.[279]

---

[270] Senior Vice President of Product Security Interview (Aug. 30, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018).
[271] Former CIO Interview (Oct. 31, 2018).
[272] Former Countermeasures Manager Interview (Sept. 12, 2018). The Countermeasures team had already begun taking several steps in response to the Apache Struts vulnerability prior to the March 16 meeting. *See* Part IV.E.
[273] EFXCONG-PSI000023034.
[274] EFXCONG-PSI000036371–72.
[275] *Id.* The former GTVM Director indicated that Aitor de la Cruz reached this conclusion after reviewing the release notes from Apache. Former GTVM Director Interview (Aug. 19, 2018).
[276] EFXCONG-PSI000036371–72.
[277] Briefing with Equifax (Mar. 27, 2018).
[278] *Id.*
[279] *Id.*

The GTVM Director stated that application owners were added to the GTVM list after the breach.[280] The company also stressed that it is difficult for managers to ensure their team members are receiving appropriate alerts.[281] Instead, GTVM highlighted the vulnerability in its monthly slide deck and accompanying meeting invite, which the developer's manager would have seen through the GTVM distribution list.[282] Developers were also responsible for subscribing to push notifications from software vendors about security vulnerabilities.[283] The application developer who was aware of the company's use of Apache Struts was not subscribed to notifications from Apache prior to the breach and did not receive any notification from Apache concerning the Apache Struts vulnerability.[284]

E. Equifax Scanned Its Systems and Servers for the Vulnerable Versions of Apache Struts and Found No Vulnerability

When Equifax receives a vulnerability notice, the security group will usually verify that a security patch is necessary.[285] Many companies facilitate this process by creating signatures to guide efforts that search for, detect, or block nefarious traffic and to detect or block such traffic.[286]

While Equifax's Countermeasures team is responsible for writing, testing, and installing signatures and rules, it is not involved in the actual patching process.[287] The processes of installing signatures and patches are "independent and de-coupled" because the security team installs signatures and rules regardless of the status of the patching process.[288] The former Countermeasures Manager explained that a rule update helps detect an intrusion while a patch addresses the vulnerability susceptible to exploitation.[289] The Countermeasures team at Equifax would install a signature or rule even if the application owner never reached out confirming a vulnerability.[290] When asked whether it was a best practice to install a signature or rule instead of patching, the Senior Vice President of Product Security stated that, "a signature is not the only thing you would do. You would try to do everything."[291]

---

[280] Former GTVM Director Interview (Aug. 19, 2018).
[281] Briefing with Equifax (Sept. 24, 2018).
[282] EFXCONG-PSI000034551; Briefing with Equifax (Mar. 27, 2018).
[283] Former CSO Interview (Oct. 4, 2018).
[284] Email from Counsel for Equifax to Subcommittee staff (Jan. 31, 2019); Email from Counsel for Equifax to Subcommittee staff (Feb. 4, 2019).
[285] Briefing with Equifax (Sept. 24, 2018).
[286] Former Countermeasures Manager Interview (Sept. 12, 2018).
[287] *Id.*
[288] *Id.*
[289] *Id.*
[290] *Id.*
[291] Senior Vice President of Product Security Interview (Aug. 30, 2018).

The Countermeasures team at Equifax had a regular schedule for pushing signature and rule updates every two weeks on Tuesdays and Saturdays.[292] This schedule aimed to align with the release cycles of signature and rule updates from security vendors.[293] Similar to the GTVM team, they would conduct out-of-band updates for signatures and rules that could not wait until the next regularly scheduled update.[294] This could reduce the waiting time for installing a critical signature or rule to a few nights.[295]

The company received the US-CERT alert on March 8.[296] The Countermeasures Manager understood that it was possible for anyone to exploit the vulnerability, and began planning to install signature rules as soon as possible.[297] Signatures to block attempts to exploit the Apache Struts vulnerability were available on March 7 from Cisco Talos, a threat intelligence group.[298] Emerging Threats, another provider of threat intelligence, also released a signature rule on March 8.[299] The next scheduled Countermeasures update was Saturday, March 11.[300] System issues delayed the process, however, and Countermeasures instead installed the rules as part of the next scheduled update on March 14.[301]

As of March 14, Equifax believed it had the ability to detect and block attempts to exploit the Apache Struts vulnerability.[302] Prior to July 2017, GTVM ran manually configured scans of external-facing and internal networks once a month.[303] At any given time, Equifax has over 18,000 rules operating in detection mode and over 4,000 more in block mode.[304] With the signature in place to detect the Apache Struts vulnerability, the Vulnerability Assessment team ran its standard scan with a commercial scanning tool from a third-party vendor, and also consulted an additional tool to evaluate source code for potential vulnerabilities and to determine if one of the vulnerable versions of Struts was in use within the company.[305] On March 14, the Countermeasures team added new rules to the company's intrusion prevention systems, which identified and blocked a "significant

---

[292] Former Countermeasures Manager Interview (Sept. 12, 2018).
[293] *Id.*
[294] *Id.*
[295] *Id.*
[296] *Id.*
[297] *Id.*
[298] EFXCONG-PSI000033569–70.
[299] EFXCONG-PSI000033569.
[300] Former Countermeasures Manager Interview (Sept. 12, 2018); EFXCONG-PSI000023034.
[301] *Id.*
[302] Former Countermeasures Manager Interview (Sept. 12, 2018).
[303] Former GTVM Director Interview (Aug. 19, 2018). The former GTVM Director indicated that the industry mark is weekly, which suggests Equifax was below that mark prior to July 2017. Former GTVM Director Interview (Aug. 19, 2018).
[304] Former Countermeasures Manager Interview (Sept. 12, 2018).
[305] Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019); *see also* Briefing with Equifax (Sept. 24, 2018).

number of Struts [exploit attempts]" that same day.[306] The GTVM team also used another commercially available product to search for vulnerable versions of Apache Struts and found none.[307] None of Equifax's subsequent scans identified an unpatched instance of the Apache Struts vulnerability.[308] Equifax also did not discover that attackers had successfully exploited a vulnerable version of Apache Struts and gained access to the company's network for several months.[309]

F. Expired SSL Certificates Delayed Equifax's Ability to Detect the Breach for Months

SSL is "a global standard security technology that enables encrypted communication between a web browser and a web server."[310] An SSL certificate is needed to enable encryption when a user is interacting with a website.[311] Websites that use SSL certificates have a web address beginning with "https://" and often display a padlock symbol on the left side of the web address bar.[312] Millions of online businesses use SSL certificates to secure their websites.[313] From the perspective of an individual browsing the internet, an SSL certificate indicates that information sent or received through the site is private.[314]

SSL certificates also allow companies to examine encrypted network traffic.[315] Without an up-to-date SSL certificate, a company's ability to observe the attempts of bad actors who encrypt their traffic in an attempt to access a company's network is limited.[316] Larger organizations typically use certificates on an application basis rather than enterprise-wide.[317] Therefore, if an organization has 100 applications, the organization will typically need 100 corresponding certificates.[318] Although SSL certificates are typically active for one year, expiration dates can vary by application.[319] At Equifax, the Countermeasures team

---

306 Briefing with Equifax (Sept. 24, 2018).
307 Former GTVM Director Interview (Aug. 19, 2018).
308 Briefing with Equifax (Mar. 27, 2018).
309 *Id.*
310 *Everything You Need to Know About SSL Certificates*, VERISIGN, https://www.verisign.com/en_US/website-presence/website-optimization/ssl-certificates/index.xhtml.
311 *What is SSL? SSL Certificate Basics*, SSL SHOPPER (May 15, 2017), https://www.sslshopper.com/what-is-ssl.html.
312 *Id.*
313 *Id.*
314 *Check if a Site's Connection is Secure*, GOOGLE, https://support.google.com/chrome/answer/95617?hl=en; *How Do I Tell if My Connection to a Website is Secure?*, MOZILLA, https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure.
315 Briefing with Equifax (Mar. 27, 2018).
316 Former Countermeasures Manager Interview (Sept. 12, 2018).
317 Briefing with Equifax (Mar. 27, 2018).
318 *Id.*
319 *Id.*

was responsible, as of late 2016, for the actual installation, or "onboarding," of new certificates.[320]

Prior to the breach, Equifax routed inbound web traffic through a decryptor.[321] Once an SSL certificate was in place, the certificate would decrypt incoming traffic.[322] The IT department was responsible for maintaining all SSL certificates through an approach described as "individual management."[323] In other words, each individual IT employee responsible for an application was also responsible for updating a corresponding certificate.[324] The former CSO stated that it would be a good idea to have a way to track all SSL certificates and their life cycles.[325] Around 2016, the former CSO obtained the necessary funding and approval for the use of a certificate management program developed and sold by a commercial software company.[326] The process of integrating this program was in its early stages prior to the breach, and Equifax had not fully implemented it across its entire network when the breach occurred.[327] The ultimate goal was the automatic detection and notification of an expired SSL certificate through a scan.[328]

The security and IT teams at Equifax initiated a project in early 2017 to update SSL certificates.[329] Equifax developed a list of expired SSL certificates, and the Countermeasures team began onboarding new certificates over the course of that year.[330] This list included SSL certificates for sites in the United States and several foreign countries.[331] Equifax had already on-boarded hundreds of new certificates without issue prior to July 29, 2017, which was when the team planned to update the SSL certificate for the online dispute portal.[332] The Countermeasures team on-boarded a batch of seventy-four SSL certificates that evening, including the SSL certificate for the online dispute portal.[333]

Immediately after onboarding the new SSL certificate, the Countermeasures team discovered suspicious internet traffic directed from the online dispute portal to

---

[320] Former Countermeasures Manager Interview (Sept. 12, 2018).
[321] Former CSO Interview (Oct. 4, 2018).
[322] *Id.*
[323] *Id.*
[324] *Id.*
[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *Id.*
[329] Former Countermeasures Manager Interview (Sept. 12, 2018); Former CSO Interview (Oct. 4, 2018).
[330] Briefing with Equifax (Sept. 24, 2018); EFXCONG-PSI000040523.
[331] EFXCONG-PSI000040524.
[332] *Id.*
[333] Former Countermeasures Manager Interview (Sept. 12, 2018).

an IP address based in China.[334] The security team opened an investigation; the team was alarmed, in part, because Equifax does not conduct business in China and made the decision to immediately block the IP address.[335] The company observed similar traffic to another IP address that appeared to be connected to a Chinese entity on July 30, which contributed to the security team's recommendation to take down the online dispute portal that day.[336]

As discussed in further detail below, Equifax later determined that hackers first gained access to Equifax's system on May 13, 2017.[337] This means that the company's inability to decrypt and inspect incoming traffic from the online dispute portal due to the expiration of the relevant SSL certificate delayed its ability to detect the breach for seventy-eight days. According to Equifax, the SSL certificate for the online dispute portal had been expired since November 2016, eight months before it was eventually updated in late July 2017.[338]

G. Once Inside Equifax's Online Dispute Portal, the Hackers Accessed Other Equifax Databases

Between May 13 and July 30, 2017, unauthorized hackers gained access to certain files that store PII maintained by Equifax.[339] The attackers eventually accessed the online dispute portal, which allows individuals to dispute inaccurate or incomplete information on their Equifax credit report, and sent queries and commands to other systems to retrieve PII residing on other Equifax systems.[340] Their search led to a data repository containing additional PII, as well as unencrypted usernames and passwords that provided the attackers with access to several other Equifax databases.[341] During this time, the attackers removed stolen data over an encrypted connection without immediate detection.[342]

Equifax confirmed to Subcommittee staff that the Apache Struts vulnerability led to the data breach.[343] In addition to the failure to patch the Apache Struts vulnerability, three factors facilitated the data breach.[344] First, the

---

[334] Former VP of the CTC Interview (Aug. 27, 2018); Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019).
[335] *Id.*
[336] *Id.*
[337] Briefing with Equifax (Mar. 27, 2018).
[338] *Id.* The former CSO does not recall the certificate being expired and believed this was a new certificate. Former CSO Interview (Oct. 4, 2018).
[339] Briefing with Equifax (Sept. 20, 2017); *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.
[340] Briefing with Equifax (Mar. 27, 2017).
[341] *Id.*
[342] *Id.*
[343] *Id.*
[344] *Id.*

hackers could access credentials for certain other databases and applications because some Equifax employees saved those credentials on a file share.[345] Second, once the hackers gained access, they could access certain databases because of a lack of network segmentation within the relevant environment.[346] Such network segmentation restricts unnecessary access to other systems once a user is inside a particular environment, such as the dispute portal.[347] The lack of segmentation was a conscious decision by Equifax to support efficient business operations and functionality over security protocols.[348] Finally, at the time of the breach, Equifax also did not have basic tools or processes in place to detect and identify changes to files accessible through the online dispute portal application or the corresponding web servers.[349] This type of cybersecurity monitoring would have generated real-time alerts and detected any unauthorized changes made by the hackers.[350]

H. Equifax Waited Six Weeks to Inform the Public of the Breach

Immediately after onboarding the new SSL certificate on July 29, the Countermeasures team discovered suspicious inbound internet traffic directed from the online dispute portal to an IP address based in China; the company made the decision to immediately block the associated IP address.[351] The company observed similar traffic to another IP address that appeared to be connected to a Chinese entity on July 30, which contributed to the security team's recommendation to take down the online dispute portal that day.[352] On July 31, the then-CIO told Richard Smith, then-Chief Executive Officer, that the security team had discovered a security incident and taken down the online dispute portal.[353]

On August 2, Equifax retained the law firm King & Spalding LLP ("King & Spalding").[354] King & Spalding engaged the independent cybersecurity forensic consulting firm Mandiant to investigate the suspicious activity.[355] In addition, Equifax contacted the Federal Bureau of Investigation ("FBI") to report the suspicious activity.[356] Over the next several weeks, Mandiant and select Equifax employees analyzed forensic data seeking to identify and understand the unauthorized activity on the network.[357] By August 11, Mandiant and Equifax had

---

[345] *Id.*
[346] *Id.*
[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] *Id.*
[351] Former VP of the CTC Interview (Aug. 27, 2018); Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019).
[352] *Id.*
[353] Former CIO Interview (Oct. 31, 2018).
[354] Briefing with Equifax (Sept. 20, 2017).
[355] EFXCONG-PSI000036879.
[356] Briefing with Equifax (Sept. 20, 2017).
[357] *Id.*

determined that, in addition to documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumer PII, and potentially other data tables.[358]

On August 15, Richard Smith was informed that it appeared consumer PII had likely been stolen.[359] On August 17, Smith held a senior leadership team meeting to receive a detailed briefing on the investigation into the incident.[360] On August 22, Equifax instituted a legal hold requiring the suspension of its document retention policy to prevent the destruction of any documents related to the breach.[361] On this same day, Smith notified the Presiding Director of Equifax's Board of Directors, Mark Feidler, of the data breach, as well as the individuals who reported directly to him who led Equifax's various business units.[362] In telephonic board meetings on August 24 and 25, the full Board of Directors learned of the breach.[363] Equifax also began developing remedial solutions to assist affected consumers.[364] On September 1, Smith convened a Board meeting to discuss the scale of the breach and what he had learned up to this point from the investigation.[365] The Board discussed efforts to develop a notification and remediation program that would help consumers deal with the potential results of the incident.[366]

By September 4, the investigative team had created a list of approximately 143 million consumers whose personal information Equifax believed the attackers had stolen.[367] Equifax kept the FBI informed of its progress and significant developments in the investigation.[368] On September 7, 2017, Equifax publicly announced the breach through a nationwide press release.[369] The release indicated that the breach involved PII for 143 million U.S. consumers, including names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers.[370] On October 2, 2017, Equifax announced that the breach may have involved PII for approximately 2.5 million additional U.S. consumers, for a

---

[358] *Id.*
[359] Email from Counsel for Equifax to Subcommittee staff (Jan. 28, 2019).
[360] *Id.*
[361] Email from Counsel for Equifax to Subcommittee staff (Oct. 1, 2018).
[362] Email from Counsel for Equifax to Subcommittee staff (Jan. 28, 2019).
[363] *Id.*
[364] *Id.*
[365] *Id.*
[366] *Id.*
[367] Briefing with Equifax (Sept. 20, 2017).
[368] *Id.*
[369] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.
[370] *Id.*

total of 145.5 million people.[371] On March 1, 2018, Equifax announced that it had identified approximately 2.4 million additional U.S. consumers whose names and partial driver's license information were also stolen in the breach, but who had not been previously identified in the company's prior disclosures about the incident.[372]

Other entities that have suffered data breaches have waited for varying periods of time before notifying the public. For example, some companies have disclosed data breaches in days.[373] Other companies have taken years to notify the public or decided against notifying the public at all.[374]

1. Some Companies Have Disclosed Data Breaches Days After Discovering Them

Target, one of the largest retail chains in the United States, suffered a data breach in 2013.[375] Intruders breached Target's computer system on November 12, 2013.[376] The company's security systems detected suspicious activity that same day.[377] However, the company did not realize a data breach had occurred until the Department of Justice contacted Target one month later, on December 12, 2013.[378] Seven days later, on December 19, 2013, Target made a public announcement of the breach.[379] During the breach, hackers obtained credit and debit card information for about 40 million customers.[380] Several weeks after announcing the breach, Target "said that other information for 70 million people, including email and mailing addresses, had also been exposed."[381] Target eventually paid $18.5 million to 47 states and the District of Columbia as part of a settlement with state attorneys general over the breach and compromised data.[382]

---

[371] *Equifax Announces Cybersecurity Firm has Concluded Forensic Investigation of Cybersecurity Incident*, EQUIFAX (Oct. 2, 2017), https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821.
[372] *Equifax Releases Updated Information on 2017 Cybersecurity Incident*, EQUIFAX (Mar. 1, 2018), https://investor.equifax.com/news-and-events/news/2018/03-01-2018-140531340.
[373] *See infra* Part IV.H.1.
[374] *See infra* Part IV.H.2.
[375] N. ERIC WEISS AND RENA S. MILLER, CONG. RESEARCH SERV., R43496, THE TARGET AND OTHER FINANCIAL DATA BREACHES: FREQUENTLY ASKED QUESTIONS 2 (2015).
[376] *Id.*
[377] *Id.*
[378] *Id.*
[379] *Id*. at 3.
[380] Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.
[381] *Id.*
[382] *Id.*

In April 2014, hackers gained access to the network of another large retail chain, Home Depot, and remained undetected for five months.[383] Home Depot eventually learned that hackers compromised the account information of 56 million cardholders – the largest known breach of a retail company's computer network at the time.[384] Home Depot's investigation began on September 2, 2014, and they provided an initial public notification six days later on September 8, 2014.[385] In March 2017, Home Depot agreed to pay $25 million for damages "incurred as a result of the breach, one of the biggest in history."[386] The settlement also required Home Depot "to tighten its cyber-security practices and to subject its vendors to more scrutiny."[387]

Anthem, one of the nation's largest health insurers suffered a data breach in 2015.[388] Anthem detected the breach on January 29, 2015.[389] Hackers were able to "breach a database that contained as many as 80 million records of current and former customers" and employees.[390] The database contained "names, Social Security numbers, birthdays, addresses, email, and employment information, including income data."[391] Anthem notified the public eight days later on February 5, 2015.[392]

Anthem agreed to a $115 million settlement that also required Anthem to provide victims "a minimum of two years of credit monitoring and identity theft protection, cash instead of credit monitoring for those who can show they already have a credit monitoring service, and reimbursement of out-of-pocket costs traceable to the data breach."[393] In addition, the settlement required Anthem to improve "its information security practices to protect personal information stored on its databases."[394] This included "archiving databases with strict access controls and monitoring requirements, strengthening various data security controls, encrypting

---

[383] Nicole Perlroth, *Home Depot Says Data from 56 Million Cards Was Taken in Breach*, N.Y. TIMES (Sept. 18, 2014), https://bits.blogs.nytimes.com/2014/09/18/home-depot-says-data-from-56-million-cards-taken-in-breach.
[384] *Id.*
[385] *The Home Depot Provides Update on Breach Investigation*, THE HOME DEPOT (Sept. 8, 2014), http://ir.homedepot.com/news-releases/2014/09-08-2014-014517970.
[386] Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, FORTUNE (Mar. 9, 2017), http://fortune.com/2017/03/09/home-depot-data-breach-banks.
[387] *Id.*
[388] Reed Abelson and Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 5, 2015), https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html.
[389] *Id.*
[390] *Id.*
[391] *Id.*
[392] *Id.*
[393] Fred Donovan, *Judge Gives Final OK to $115M Anthem Data Breach Settlement*, HEALTH IT SECURITY (Aug. 20, 2018), https://healthitsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement.
[394] *Id.*

sensitive information, and guaranteeing a certain level of funding for Anthem's information security."[395] In October 2018, Anthem agreed to pay the U.S. government $16 million to settle potential privacy violations stemming from the cyber hack.[396] The settlement between Anthem and the Department of Health and Human Services "represents the largest amount collected by the agency in a health care data breach."[397]

2. Other Companies Made Public Disclosure Years Later or Simply Declined to Notify

In recent years, Yahoo! has suffered two data breaches. The first breach took place around August 2013.[398] Yahoo! initially believed the 2013 breach affected over 1 billion user accounts.[399] Yahoo! later confirmed that the 2013 breach impacted all 3 billion of its user accounts.[400] The impacted data included names, birth dates, telephone numbers, passwords, security questions and answers, and backup email addresses.[401] The second breach occurred sometime in late 2014 and affected over 500 million Yahoo! user accounts.[402]

Yahoo! did not disclose the 2013 breach until December 2016, after negotiating their sale to Verizon Communications.[403] The public did not learn the full extent of the 2013 breach until October 2017.[404] In April 2018, the Securities and Exchange Commission announced a $35 million fine against Yahoo!, now known as Altaba, for failing to tell investors about the cyber breach for two years.[405] This fine represented the first time the regulator punished a company for such

---

[395] *Id.*
[396] Ricardo Alonso-Zalvidar, *Insurer Anthem will Pay Record $16M for Massive Data Breach*, THE ASSOCIATED PRESS (Oct. 15, 2018), https://www.apnews.com/591ed32303df48c0b3f86358fe8a58eb.
[397] *Id.*
[398] Vindu Goel and Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.
[399] *Id.*
[400] Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.
[401] *Id.*
[402] Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.
[403] Vindu Goel and Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.
[404] Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.
[405] Renae Merle, *Yahoo Fined $35 Million for Failing to Disclose Cyber Breach*, THE WASHINGTON POST (Apr. 24, 2018), https://www.washingtonpost.com/news/business/wp/2018/04/24/yahoo-fined-35-million-for-failing-to-disclose-cyber-breach/?utm_term=.1f8827362e5b.

conduct.[406] Moreover, Yahoo! agreed to pay up to $85 million to settle consumer actions brought as a result of the two data breaches.[407]

In October 2018, Google announced that its Google+ network had a security vulnerability that left users' private profile data exposed to third-party applications.[408] The data breach may have impacted up to 500,000 Google+ accounts.[409] Google discovered and patched the vulnerability in March 2018 but did not notify users of the security issue because it did not appear that anyone had gained access to user information.[410] Google reportedly opted not to disclose this data breach due to a fear of drawing regulatory scrutiny and suffering reputational damage.[411]

I. Several Current and Former Senior Equifax Employees Believe Equifax Acted Appropriately in Responding to the Apache Struts Vulnerability

As part of each interview it conducted, the Subcommittee asked current and former Equifax employees to assess Equifax's response to the March 2017 Apache Struts vulnerability.[412] The Subcommittee sought to understand whether the cybersecurity breach was the result of a failure to follow established policies or a failure to develop effective policies. The responses of these current and former employees varied, but as explained below, most believed that the security team acted appropriately in responding to the vulnerability.

The former Director of the GTVM team served from 2014 to 2017.[413] He stressed that his team worked hard to be transparent and disseminate vulnerability

---

[406] *Id.*
[407] Amanda Bronstad, *Yahoo Agrees to Pay $85M to Settle Consumer Data Breach Class Actions*, THE RECORDER (Oct. 23, 2018), https://www.law.com/therecorder/2018/10/23/yahoo-agrees-to-pay-85m-to-settle-consumer-dat-breach-class-actions/?slreturn=20180929154224.
[408] Daisuke Wakabayashi, *Google Plus Will be Shut Down After User Information Was Exposed*, N.Y. TIMES (Oct. 8, 2018), https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html.
[409] Ben Smith, *Project Strobe: Protecting Your Data, Improving Our Third-Party APIs, and Sunsetting Consumer Google+*, GOOGLE (Oct. 8, 2018), https://www.blog.google/technology/safety-security/project-strobe.
[410] Daisuke Wakabayashi, *Google Plus Will be Shut Down After User Information Was Exposed*, N.Y. TIMES (Oct. 8, 2018), https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html.
[411] Douglas MacMillan and Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, THE WALL ST. J. (Oct. 8, 2018), https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194.
[412] Former GTVM Director Interview (Aug. 19, 2018); Former VP of the CTC Interview (Aug. 27, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Former Countermeasures Manager Interview (Sept. 12, 2018); Former CSO Interview (Oct. 4, 2018); Former CIO Interview (Oct. 31, 2018).
[413] Former GTVM Director Interview (Aug. 19, 2018).

information across the company.[414] He noted that over 400 people received GTVM notices each month.[415] The former GTVM Director described the process his team followed in response to the Apache Struts vulnerability as "effective" and "reputable and we were working to improve the process."[416] He believed it was hard to say whether Equifax could have avoided the breach, and he indicated that other cybersecurity professionals working at other companies believed "that could have been us."[417] The former GTVM Director stated that after the breach, "instead of us reaching out, people started reaching out to us. There was a lot of additional vulnerability work." When asked whether this was not the thinking before the breach, the former GTVM Director responded that "security wasn't first" and that "the event made everyone focus on it more."[418] When asked what grade he would assign to Equifax's data security protocols prior to the breach, he responded that he would "probably say a C especially on remediation. Especially on Apache, I would give it a C on identification and remediation."[419] He further indicated that even after the breach, he would "say still a C but getting to improvements."[420] He added that Equifax was "still getting there on [the] remediation side."[421] The former GTVM Director admitted he was a "hard grader."[422]

The former Vice President of the CTC served from September 2016 to 2017.[423] She indicated that better policies and procedures probably could have helped prevent the cybersecurity breach.[424] Despite this, she noted that Equifax security had good policies and procedures in place and had up-to-date scanning tools for vulnerability detection.[425] She stated that she was unsure if anything about the response to the March 2017 vulnerability could have been different because the security team was not part of the Development team, which was responsible for installing patches.[426] When asked what grade she would assign to Equifax's data security protocols, she responded with a "B, because nothing is an A in security."[427]

The Senior Vice President of Product Security at Equifax joined the company in 2016, and was Vice President of Security Operations and then oversaw Cyber Operations during 2017.[428] He did not believe there was one single reason for the

---

[414] *Id.*
[415] *Id.*
[416] *Id.*
[417] *Id.*
[418] *Id.*
[419] *Id.*
[420] *Id.*
[421] *Id.*
[422] *Id.*; Email from Counsel for former GTVM Director (Feb. 19, 2019).
[423] Former VP of the CTC Interview (Aug. 27, 2018).
[424] *Id.*
[425] *Id.*
[426] *Id.*
[427] *Id.*
[428] Senior Vice President of Product Security Interview (Aug. 30, 2018).

breach and declined to weigh in on whether Equifax could have prevented the breach.[429] He did not think anything in the company's cybersecurity policies was "egregiously wrong" and that his team acted appropriately even before the breach.[430] Unprompted, he stated that he has met with representatives from numerous other companies since the breach who told him a variation of "it could have been us as well."[431] He argued that Equifax was not doing anything drastically different from other companies and that many companies struggle with exactly the same cybersecurity issues as Equifax.[432] He also noted that the post-breach efforts to improve Equifax's security posture have increased.[433]

The former Countermeasures Manager at Equifax served in an acting and then permanent capacity from 2016 to 2017.[434] He believed Equifax suffered a cybersecurity breach because of a "sophisticated" and "highly motivated" adversary.[435] He added that, "if asset management was a perfect silver bullet then perhaps this may not have happened."[436] He told Subcommittee staff that he does not think the Countermeasures team could have done anything differently in response to the March 2017 vulnerability.[437] He was as surprised as anyone that Equifax suffered a breach because of the "combination of the sophistication of the attack and the talent at Equifax. We had rock stars at Equifax who were de facto pillars in the field."[438] The former Countermeasures Manager believes the response to the vulnerability was "not only defensible, but justifiable."[439]

The acting Chief Information Security Officer ("CISO") at Equifax after the breach is presently the Deputy CISO and leader of the engineering function for the security team.[440] He stated that two functionality gaps in the patch management process led to the failure to patch the Apache Struts vulnerability: "When Equifax receives a vulnerability notice, Equifax will usually validate that a patch is necessary. However, the scanning tool did not 'crawl' through the subdirectory and, thus, did not identify the vulnerability. So, when Equifax ran the scan, the company did not receive a message that the system was vulnerable."[441] The Deputy CISO acknowledged that if a scan did not reveal a vulnerability, the security team would assume a vulnerability did not exist.[442] He also added that the vulnerability

---

[429] *Id.*
[430] *Id.*
[431] *Id.*
[432] *Id.*
[433] *Id.*
[434] Former Countermeasures Manager Interview (Sept. 12, 2018).
[435] *Id.*
[436] *Id.*
[437] *Id.*
[438] *Id.*
[439] *Id.*
[440] Briefing with Equifax (Sept. 24, 2018).
[441] Briefing with Equifax (Mar. 27, 2018).
[442] *Id.*

should have been patched within 48 hours, that Equifax has addressed both functionality gaps and the issues in the 2015 patching audit, and that since the breach, Equifax's new motto is "security over service."[443]

The former CSO of Equifax served from 2013 to 2017.[444] In mid-July 2017, she submitted a request to retire at the end of 2017, after a 35-year career in IT; Equifax granted her request in September 2017.[445] The former CSO indicated that she felt "very sad" after learning about the breach on July 29 because she knew this was a very "unfortunate event."[446] She believed the security team did its job in responding to the vulnerability.[447] The former CSO added that she assumed the IT department had patched the vulnerable versions of Apache Struts because the scans never identified a vulnerability.[448]

The former CIO of Equifax served from 2010 to 2017.[449] In early 2017, the former CIO communicated his intention to retire that year.[450] Shortly after Equifax publicly announced the breach in September 2017, Richard Smith asked the former CIO to retire that month, which he agreed to do but described his decision as "not voluntary."[451] Despite overseeing the department responsible for installing software applications and patching, the former CIO first learned of the breach on August 17, nineteen days after Equifax discovered it.[452] (The former CIO did, however, learn of a security-related incident involving the dispute portal on July 30, 2017.[453]) The former CIO further informed the Subcommittee that he was never made aware of the March 2017 Apache Struts vulnerability, even after the US-CERT and GTVM alerts on March 8 and March 9, 2017.[454] The former CIO also stated that he was not surprised to learn of the breach so late because the company had a "need to know" philosophy in the context of a security incident: "It is just the way we operate on principle."[455] The former CIO described the breach as a "very unfortunate situation and added that he did not understand why the vulnerability

---

[443] *Id.*
[444] Former CSO Interview (Oct. 4, 2018).
[445] The former CSO also indicated that she was Chief Privacy Officer but the "role was operationally focused" and she understood her responsibilities to include "privacy operations, reviewing contracts for privacy language, and reviewing policy updates." *Id.*
[446] *Id.*
[447] *Id.*
[448] *Id.*
[449] Former CIO Interview (Oct. 31, 2018).
[450] *Id.*
[451] *Id.*
[452] *Id.*
[453] Email from Counsel for the former CIO to Subcommittee staff (Feb. 20, 2019).
[454] Former CIO Interview (Oct. 31, 2018).
[455] *Id.*

"was not caught."[456] He does not think Equifax could have done anything differently.[457]

IV. EQUIFAX'S LARGEST COMPETITORS, TRANSUNION AND EXPERIAN, WERE ABLE TO QUICKLY IDENTIFY WHERE THEY WERE RUNNING VULNERABLE VERSIONS OF APACHE STRUTS AND PROACTIVELY BEGAN PATCHING

The Subcommittee reviewed the steps taken by TransUnion and Experian in response to the Apache Struts vulnerability that facilitated the Equifax breach. The following information reflects the steps taken by each company pursuant to the policies and procedures that were in place when US-CERT announced the Apache Struts vulnerability in March 2017. Neither company announced that they had suffered a data breach as a result of a successful exploitation of the Apache Struts vulnerability.

A. CRAs Had Different Timelines for Patch Management

TransUnion and Experian's policies required patching vulnerabilities in their systems to within certain timeframes.

1. TransUnion

TransUnion's Patch Management Standards policy identified several different categories of patches, such as emergency patches, requiring remediation within a week and critical patches requiring remediation within two weeks:[458]

Patch Category	Patch Deployment Times
Operating System Emergency	Within seven days
Operating System Critical	Within two weeks
Third Party Application Emergency	Within seven days
Third Party Application Critical	Within one month

The U.S. Information Technology Division at TransUnion ("USIT") was responsible for patching and updating applications.[459] Division employees used Patch Management Systems to maintain patches for servers having databases that contained confidential, private, or sensitive data.[460] It was the responsibility of USIT and the Distributed Systems Integration Group ("DSI") to "maintain an inventory of systems at TransUnion, including those that are patched or not

[456] *Id.*
[457] *Id.*
[458] TU-PSI-00000461.
[459] TU-PSI-00000462.
[460] TU-PSI-00000463.

patched."[461] In addition, USIT and DSI were responsible for performing "regular scans to determine the state of patches on systems at TransUnion."[462] The USIT and Security Department worked together for patch installation.[463] The Security Department identified where a patch was necessary, and USIT installed them.[464]

TransUnion used commercial software to verify installation of a patch, which scanned the network every week.[465] In addition, TransUnion fed the scanning data into a tool that created risk meters and dashboards.[466] Owners of assets could view vulnerabilities and scores of those assets.[467] The tool informed owners of assets if the vulnerability was easy to exploit.[468] Once TransUnion scanned and found an issue, it tracked the issue through closure.[469]

2. Experian

According to Experian's policies, all vulnerabilities associated with Experian's IT facilities required remediation within the following timeframes:[470]

Vulnerability Priority	Resolved Within (external/extranet facing)
Significant (critical)	15 days
High	30 days

Application vulnerabilities had a separate timeframe:[471]

Application Risk Criticality		Flaw/Vulnerability Severity Not Allowed + Calendar Days to Remediate Flaw/Vulnerability	
Site Facing	Data Classification	Critical	High
Internet + Extranet	Restricted + Confidential + Internal + Public	30 days	60 Days

[461] TU-PSI-00000464.
[462] *Id.*
[463] Briefing with TransUnion (Oct. 22, 2018).
[464] *Id.*
[465] Briefing with TransUnion (Mar. 29, 2018).
[466] *Id.*
[467] *Id.*
[468] *Id.*
[469] *Id.*
[470] PSI_00001015.
[471] PSI_00001100.

Experian business units were responsible for installing patches.[472] The information security team managed all of the information regarding security vulnerabilities centrally.[473] Experian implemented patches using a combination of manual and automated processes.[474] To verify the successful installation of a patch, Experian used a tool to scan for the presence of a known vulnerability.[475] In addition, Experian used a commercial product to scan applications to ensure successful patch implementation.[476]

Experian treated critical vulnerabilities differently than other vulnerabilities.[477] Critical vulnerabilities, such as the Apache Struts vulnerability, went through Experian's crisis management process, which often involved multiple meetings per day and regular tracking reports.[478]

B. CRAs Generally Performed Vulnerability Scans on a Regular Basis

TransUnion and Experian frequently scanned their systems for vulnerabilities using various tools.

1. TransUnion

TransUnion's information security team scanned all known assets on a weekly basis using software from various vendors.[479] Every week, TransUnion would also conduct a full re-scan of its environment.[480] As part of this process, the company performed application and vulnerability scanning.[481] The vulnerability scans ran on an automated schedule globally every day.[482] The scanning tools looked for signatures associated with known vulnerabilities.[483] TransUnion also deployed signature and non-signature based tools to detect and block suspicious activity.[484] TransUnion also pushed all of the previous day's scan results to software that acted as an organizational, tracking, and visualization tool for scan

---

[472] Briefing with Experian (Nov. 9, 2018); Email from Counsel for Experian to Subcommittee staff (Feb. 20, 2019).
[473] *Id.*
[474] *Id.*
[475] *Id.*
[476] *Id.*
[477] *Id.*
[478] *Id.*
[479] TU-PSI-00000770; Letter from TransUnion to the Subcommittee (Aug. 6, 2018).
[480] Briefing with TransUnion (Mar. 29, 2018).
[481] Letter from TransUnion to the Subcommittee (Aug. 6, 2018).
[482] Briefing with TransUnion (Mar. 29, 2018).
[483] *Id.*
[484] Briefing with TransUnion (Oct. 22, 2018).

results.[485] Each asset owner was responsible for reviewing vulnerability information for the assets they were responsible for at least once a week.[486]

2. Experian

The Enterprise Vulnerability Management Team or a commercially-available solution approved by the Global Security Office conducted Experian's vulnerability scanning.[487] Experian used commercial scanning software as an agent on many endpoints across its network.[488] Experian required that the scans be based on industry best practices using vendor provided signatures or as dictated by other compliance requirements such as the Payment Card Information Digital Signature Standard.[489] The team scanned IP addresses that were publicly available, such as devices located in Experian data centers or colocation facilities that are accessible from the internet every seven days.[490] Externally, Experian ran daily network scans.[491]

C. Other CRAs Maintained an IT Asset Inventory

TransUnion and Experian had policies regarding the creation of an IT asset inventory to keep track of all applications, hardware, and software used in their systems.

1. TransUnion

TransUnion's Security Policy required the documentation of all information assets.[492] A designated Data Owner was responsible for the security of information assets.[493] TransUnion has maintained a comprehensive IT asset inventory for over three years.[494] The inventory includes both virtual and physical assets.[495]

2. Experian

Experian's policy required a current inventory of the company's information assets, including hardware, software, applications, and licenses.[496] The Information

---

[485] TU-PSI-00000760.
[486] *Id.*
[487] PSI_00000466.
[488] Briefing with Experian (Nov. 9, 2018).
[489] PSI_00000466; *Computer Security Resource Center*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, https://csrc.nist.gov/glossary/term/DSS.
[490] PSI_00000467.
[491] Briefing with Experian (Nov. 9, 2018).
[492] TU-PSI-00000493.
[493] TU-PSI-00000492.
[494] Briefing with TransUnion (Oct. 22, 2018).
[495] *Id.*
[496] PSI_000001016.

Steward was responsible for maintaining an inventory of information assets, any changes in status, and/or any new applications.[497] The Information Steward was also responsible for revalidating the data inventory periodically.[498] Configuration information repositories were also required for critical information assets related to each information system.[499] Included in the repository was the current location of the asset.[500] Software assets included applications and application software.[501]

D. CRAs Lacked Written Policies for Tracking the Validity of SSL Certificates

TransUnion and Experian used SSL certificates on an application basis, meaning each application used one or more certificates. Neither company had formal, written policies addressing the management of SSL certificates in 2017.

1. TransUnion

TransUnion did not have a formal, written policy relating to SSL certificates.[502] Instead, TransUnion's CISO said that the company used a process to issue certificate authorities which followed industry best practices while acknowledging that they "don't have a centralized process."[503] Each development team was responsible for its application usage and tracked its inventory, certificate start and end dates, and the type of certificates.[504] TransUnion also uses security products that scan the company's external presence for potential issues, including expired certificates, which are tracked to closure.[505] TransUnion tried to balance the amount of time a certificate was valid, since it was impractical to reissue certificates on a daily basis or have certificates that never expired.[506]

2. Experian

Experian did not have a formal, written policy relating to SSL certificates but tracked SSL certificates manually.[507] Experian's timeframe for updating its certificates varied depending on third-party requirements and internal standards.[508] The amount of time a certificate was valid also varied.[509]

---

[497] *Id.*
[498] *Id.*
[499] *Id.*
[500] *Id.*
[501] *Id.*
[502] Briefing with TransUnion (Oct. 22, 2018).
[503] *Id.*
[504] *Id.*
[505] *Id.*
[506] Briefing with TransUnion (Mar. 29, 2018).
[507] Letter from Experian to the Subcommittee (Oct. 26, 2018).
[508] Briefing with Experian (Apr. 11, 2018).
[509] *Id.*

E. Equifax's Two Largest Competitors, TransUnion and Experian, Avoided a Cybersecurity Breach

Each CRA responded to the Apache Struts vulnerability announcement by employing similar actions. However, only TransUnion and Experian were able to identify the instances of the vulnerable version of Apache Struts running in their systems, which allowed them to successfully apply patches.

1. TransUnion

TransUnion's Threat and Intelligence team received notifications about the Apache Struts vulnerability from the Financial Services Information Sharing and Analysis Center and commercial intelligence services during the week it was announced.[510] TransUnion considered the Apache Struts vulnerability critical.[511]

Shortly after TransUnion learned of the vulnerability, it began scanning its IT assets to identify vulnerable versions of Apache Struts on its network.[512] The IT asset inventory helped TransUnion understand who was an asset owner, so the company could contact the appropriate people and the asset owners could begin developing a plan for patching.[513] TransUnion's CISO stated that the commercial scanners had difficulty detecting the Apache Struts vulnerability.[514] He pointed out that "it was widely known [in 2017] that standard software was having trouble detecting Struts."[515]

TransUnion's Information Security personnel started to review the ongoing scan results looking for vulnerable version of Apache Struts.[516] Based on this review, especially reviews of unauthenticated vulnerability scans, TransUnion identified third-party software on the TransUnion network utilizing the vulnerable version of Apache Struts.[517] TransUnion's initial vulnerability scan did not identify a large number of assets exposed to the vulnerability.[518] The company concluded, based on the information available at the time and the results of its vulnerability scanning, that the risk presented by the vulnerability was limited.[519]

---

[510] Letter from TransUnion to the Subcommittee (Aug. 6, 2018).
[511] Briefing with TransUnion (Mar. 29, 2018).
[512] Briefing with TransUnion (Oct. 22, 2018).
[513] *Id.*
[514] *Id.*
[515] *Id.*
[516] Letter from TransUnion to the Subcommittee (Aug. 6, 2018).
[517] *Id.*
[518] Letter from TransUnion to the Subcommittee (June 20, 2018).
[519] *Id.*

TransUnion used three tools to protect its systems while waiting for a patch. First, the company used a web application firewall to block attempted attacks from unauthorized parties.[520] After receiving notice of the Apache Struts vulnerability, TransUnion ensured the firewalls were in place and configured them to recognize and block Apache Struts attacks.[521] TransUnion also used an intrusion prevention system to block attacks as well as an intrusion detection system to monitor its network and issue alerts on malicious attacks.[522] Deploying these tools took weeks.[523]

TransUnion was able to patch certain Apache Struts vulnerabilities on its network within a few days of the vulnerability announcement, while others took longer.[524] TransUnion completed patching, replacing, decommissioning, or otherwise fully addressing all vulnerable versions of Apache Struts on its systems by August 2018.[525] TransUnion told the Subcommittee that there were several reasons why the process took sixteen months.[526] Some products had embedded Apache Struts, which required the vendor to produce the patch.[527] There were also a large number of patches, some of which required significant testing, working with vendors, and coordinating with customers for feedback.[528] Consequently, TransUnion spread out its patching process.[529] Some of the locations where TransUnion was running the vulnerable version of Apache Struts were not externally facing, meaning they were at a significantly reduced risk for attack because they were not exposed publicly.[530]

2. Experian

On March 9, 2017, the Experian Global Security Office Security Threat Advisory distribution list, which contains all security and operational leaders within Experian, received a Global Security Operations Center Threat Advisory.[531] Experian then used crisis management protocols to determine a plan to address the vulnerability.[532] Experian considered the vulnerability "above critical."[533] After receiving the notice, Experian used a third-party tool to scan for and identify risks

---

[520] Briefing with TransUnion (Mar. 29, 2018); Letter from TransUnion to the Subcommittee (Aug. 6, 2018).
[521] *Id.*
[522] *Id.*
[523] *Id.*
[524] Briefing with TransUnion (Oct. 22, 2018).
[525] *Id.*
[526] *Id.*
[527] Briefing with TransUnion (Mar. 29, 2018).
[528] Briefing with TransUnion (Oct. 22, 2018).
[529] *Id.*
[530] *Id.*
[531] Letter from Experian to the Subcommittee (Oct. 26, 2018).
[532] Briefing with Experian (Nov. 9, 2018).
[533] Briefing with Experian (Apr. 11, 2018).

listed in open source libraries to determine the presence of third-party vulnerabilities on its network.[534] By performing this scan, Experian determined which of its applications were running the vulnerable versions of Apache Struts.[535]

Similar to TransUnion, Experian installed a signature on a firewall to block Apache Struts attacks.[536] In addition, Experian created a custom, blocking signature, which the company replaced approximately one day later with another signature provided by a third-party vendor.[537] Experian implemented these tools within two days of the vulnerability announcement.[538]

Experian contracted a software security firm to do a targeted vulnerability scan for Struts vulnerabilities.[539] The firm conducted the scan on March 16, 2017, and a complete report was available on March 23, 2017.[540] It found an Experian server was running the vulnerable version of Struts that was exploitable.[541] The recommended remediation was to "[u]pgrade Apache struts [sic] to the latest version."[542] The report marked the finding "as closed, as the port ha[d] been firewalled off and [was] no longer accessible from the Internet."[543]

Applications based in the United States were "fully remediated" by October 24, 2017.[544]

V. EQUIFAX FAILED TO PRESERVE A COMPLETE RECORD OF EVENTS SURROUNDING THE BREACH

As part of its investigation, the Subcommittee requested several categories of documents from Equifax, including documents related to any report or analysis by Equifax concerning the 2017 breach. This request encompassed findings concerning how the breach occurred, any system vulnerabilities and mitigation efforts, and any explanation as to why the breach went undetected for months.[545] The Subcommittee made clear to Equifax's counsel that this request included communications in any form. In response, Equifax produced over 43,000 pages of documents to the Subcommittee, including email communications.

---

[534] Letter from Experian to the Subcommittee (Oct. 26, 2018).
[535] *Id.*
[536] *Id.*
[537] *Id.*
[538] *Id.*
[539] PSI_00000956-67.
[540] *Id.*
[541] *Id.*
[542] *Id.*
[543] *Id.*
[544] Letter from Experian to the Subcommittee (Oct. 26, 2018).
[545] Letter from Chairman Rob Portman and Ranking Member Tom Carper to Richard F. Smith, Chairman and Chief Executive Officer, Equifax Inc. (Sept. 13, 2017).

During interviews of both current and former Equifax employees, the Subcommittee learned that members of the security team and others commonly used Microsoft Lync ("Lync"), an instant messaging application, to communicate internally on a daily basis about Equifax business matters.[546] According to the former GTVM Director, Lync was a convenient means of communication because Equifax employees worked from various locations instead of at one central office.[547] Equifax employees indicated that they frequently used Lync for substantive discussions related to security vulnerabilities, including the events surrounding the discovery of the 2017 data breach.[548]

After learning of this application's widespread use, the Subcommittee asked to review Lync instant message records. Counsel for Equifax then told the Subcommittee that Equifax did not require employees to retain these communications until September 15, 2017, when the company changed the default setting on the platform to begin archiving chats for certain custodians.[549] This is more than six weeks after the breach was discovered, and more than three weeks after an initial legal hold went into place on August 22, 2017.[550] Because Equifax did not require employees to retain these records, the Subcommittee was unable to review all Equifax employee communications through Lync during and immediately following the discovery of the 2017 breach. Since Equifax employees told the Subcommittee they discussed the discovery of the 2017 data breach over Lync, this leaves the Subcommittee with an incomplete record.

A. Equifax's Document Retention Policy

Equifax's document retention policy in place at the time of the breach defines a "record" as: "any document, data, or recorded information, regardless of medium or characteristics, that is written or recorded *in the course of company business activity*."[551] The policy applied broadly to "records in all forms" whether "written, stored electronically, transmitted by post or electronic means, shown on films, cameras, projectors, interactive media, text messages, or spoken that require retention due to legal, regulatory, business, government or other requirements."[552]

1. Equifax's Document Retention Schedule

---

[546] Former GTVM Director Interview (Aug. 19, 2018); Former VP of the CTC Interview (Aug. 27, 2018); Senior Vice President of Product Security Interview (Aug. 30, 2018); Briefing with Equifax (Sept. 24, 2018); Former CSO Interview (Oct. 4, 2018).
[547] Former GTVM Director Interview (Aug. 19, 2018).
[548] *Id*; Former VP of the CTC Interview (Aug. 27, 2018).
[549] Email from Counsel for Equifax to Subcommittee staff (Sept. 5, 2018).
[550] Email from Counsel for Equifax to Subcommittee staff (Oct. 1, 2018).
[551] EQUIFAX, DOCUMENT RETENTION POLICY (Mar. 2017) (on file with Equifax).
[552] *Id.*

To assist Equifax employees in determining which documents they must preserve, the company established a records retention schedule, which identified records by category and their corresponding retention period.[553] Consistent with that requirement, all record owners must keep records except those defined as "disposable" under the policy.[554] According to the policy, disposable records include: "all information and documents that are temporary in nature and that have no legal or regulatory retention requirements and otherwise have been determined not to have sufficient business importance to retain for an extended period."[555]

According to the policy, examples of disposable records include items like personal correspondence, copies, and drafts of letters.[556] The policy states that disposable records are not subject to any minimum retention period.[557] The document retention policy is suspended, however, for emails and all other documents if those documents are subject to a "legal hold."[558]

2. Equifax's Legal Hold Policy

Under Equifax's policy, a legal hold requires "the suspension of policy to protect information, assets, and records in any form or medium that are subject to, or potentially subject to, pending, threatened, or imminent litigation, government investigation, audit, or other important legal or regulatory matters."[559] When Equifax's legal department issues a legal hold, record owners receive a written notice from a policy manager that details specific information about the subject matter and scope of the legal hold in question.[560] Once an employee receives a legal hold notice, Equifax's policy requires that they preserve all documents subject to the hold in their original format.[561] The policy states that under no circumstance should "any user destroy or alter records in contemplation of any matter or case, or with the intent to impair the record."[562]

Equifax discovered the data breach on July 29, 2017. An initial legal hold to retain all relevant documents related to the breach went into effect on August 22, 2017, and was distributed to additional individuals on a rolling basis, as those individuals were identified as potentially having relevant information.[563] Equifax stated that the company began archiving Lync chats on September 15, 2017, in

---

[553] *Id.*
[554] *Id.*
[555] *Id.*
[556] *Id.*
[557] *Id.*
[558] *Id.*
[559] *Id.*
[560] *Id.*
[561] *Id.*
[562] *Id.*
[563] Email from Counsel for Equifax to Subcommittee staff (Oct. 1, 2018).

response to anticipated claims and litigation on the data breach.[564] From July 29 to September 15, 2017, Equifax considered Lync messages as disposable under its document retention policy even though they contained substantive communications about the data breach "recorded in the course of company business activity."[565]

B. Equifax's Use of Lync

Lync is an application used by over 19,000 companies worldwide, according to one outside marketing company.[566] In the United States alone, there are well over 9,000 companies that currently use Lync, accounting for roughly 47 percent of Lync customers globally.[567] While different versions of Lync exist, Equifax, through its counsel, confirmed it used Lync Server 2010.[568]

Lync is most popular in the computer software industry, but a significant number of companies in the financial services industry also use it.[569] From a capability standpoint, Lync provides companies with platforms for instant messaging, audio and video calls, and online meetings.[570] Regarding the retention of chats, according to Microsoft, Lync Server 2010: "archiving is turned off by default and can be turned on by an enterprise administrator by going to the Microsoft Lync Server 2010 Control Panel Monitoring and Archiving Settings page, and updating the Archiving Policy and Archiving Configuration."[571]

C. Equifax Employees Used Lync to Discuss Business Matters, Including Events Surrounding the 2017 Data Breach

According to current and former Equifax employees, the company's employees used Lync often during routine business activities.[572] Equifax employees told the Subcommittee that they used Lync for a variety of purposes, including discussing substantive matters like the 2017 breach identification and response efforts.[573] In addition, Equifax employees did not simply use Lync to communicate

---

[564] Email from Counsel for Equifax to Subcommittee staff (Feb. 20, 2019).
[565] *Id.*; EQUIFAX, DOCUMENT RETENTION POLICY (Mar. 2017).
[566] *Companies using Microsoft Lync*, IDATALABS (2017), https://idatalabs.com/tech/products/microsoft-lync.
[567] *Id.*
[568] Email from Counsel for Equifax to Subcommittee staff (Sept. 5, 2018).
[569] *Companies Using Microsoft Lync*, IDATALABS (2017), https://idatalabs.com/tech/products/microsoft-lync.
[570] *Microsoft Lync Basic 2013*, MICROSOFT (Oct. 28, 2012), https://www.microsoft.com/en-us/download/details.aspx?id=35450.
[571] *Privacy supplement for Microsoft Lync Server 2010*, MICROSOFT (Oct. 2010), https://support.office.com/en-us/article/privacy-supplement-for-microsoft-lync-server-2010-46934364-38bf-4e94-a61b-4a6df1882db4#__toc281989604.
[572] Former GTVM Director Interview (Aug. 19, 2018); Former VP of the CTC Interview (Aug. 27, 2018).
[573] *Id.*

with colleagues on their respective teams but also to contact other employees across the company.[574] Equifax personnel continued to use Lync as the company responded to the 2017 data breach.[575] For example, Equifax's then-Director of GTVM indicated that security personnel discussed the connection between the March 2017 US-CERT notification and the suspicious network activity observed in late-July through a Lync instant message conversation.[576]

Upon learning of Equifax employees' extensive use of Lync, the Subcommittee requested copies of all internal chats containing discussions about the breach.[577] Equifax informed the Subcommittee that the company's default setting on Lync for Equifax employees did not archive chats.[578] Equifax acknowledged that they began preserving chat records on September 15, 2017, even though the company had issued a legal hold three weeks earlier, on August 22, 2017.[579] As a result, Equifax confirmed that employees did not archive copies of instant message conversations and that "chats that took place before September disappeared."[580] Equifax deemed these chats disposable records subject to no minimum retention period.[581] Counsel for Equifax confirmed that they searched chats created after September 15, 2017, but "generally did not get any hits because they were created on or after September 15, 2017 and thus post-dated the [Subcommittee] search criteria for materials created on or before September 13, 2017" [the date of the Subcommittee's request].[582]

Equifax employees who responded to the data breach told the Subcommittee that instant message conversations contained relevant information to the Subcommittee's investigation. In a subsequent production from Equifax, the company produced a seven-page transcript of one such chat.[583] This chat between two employees from the cybersecurity group spanned three days (August 1-3, 2017) and contained extensive discussion about the breach and the efforts to remediate it.[584] For example, the two Equifax employees discussed the confirmation that PII was exfiltrated; that once inside the network hackers pivoted to other internal databases; and that the March 2017 Apache Struts vulnerability caused the

---

[574] Former VP of the CTC Interview (Aug. 27, 2018).
[575] Former GTVM Director Interview (Aug. 19, 2018). Microsoft Lync was particularly convenient for employees because they discovered the breach on a weekend (July 29-30, 2017).
[576] *Id.*
[577] Telephone Call with Counsel for Equifax (Aug. 21, 2018).
[578] Email from Counsel for Equifax to Subcommittee staff (Sept. 5, 2018); Email from Counsel for Equifax to Subcommittee staff (Oct. 1, 2018).
[579] *Id.*
[580] Telephone Call with Counsel for Equifax (Aug. 28, 2018). Equifax indicated that certain chats were preserved but none were related to the Subcommittee's requests. *Id.*
[581] Telephone Call with Counsel for Equifax (Sept. 13, 2018).
[582] Email from Counsel for Equifax to Subcommittee staff (Sept. 5, 2018).
[583] EFXCONG-PSI000042562–68.
[584] *Id.*

breach.[585] The two employees also discussed how a different vulnerability detection software program would have given "instant visibility into this" activity.[586]

The Subcommittee asked Equifax to explain how the company was able to produce this record of a chat transcript, despite its claims that all chat records prior to September had been deleted.[587] Equifax explained that one of the two participants in the chat conversation must have copied the entire transcript into a separate file format, which allowed it to be retained.[588] Despite the significant substantive conversations conducted on Lync, Equifax's document retention policy considered Lync messages "disposable" and did not require employees to save their chat logs or archives. As such, from the discovery of the breach on July 29 to September 15, 2017, when the company changed the default settings, all Lync messages were automatically deleted under default Lync Server 2010 settings. Consequently, most of the Lync chats Equifax employees stated they created while discussing the data breach were deleted. Therefore, the Subcommittee was unable to review those records, and any others, documenting Equifax's real-time response to the March 2017 Apache Struts vulnerability, the July 29 discovery of the breach, and subsequent remediation efforts.

[585] *Id.*
[586] *Id.*
[587] Email from Subcommittee staff to Counsel for Equifax (Sept. 26, 2018).
[588] Email from Counsel for Equifax to Subcommittee staff (Oct. 1, 2018).