ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Equifax: America's In-Credible Insecurity

Part One: Yet Another Dragnet Surveillance Capitalist Cautionary Tale

September 2017

Authored by:

James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

Equifax: America's In-Credible Insecurity

Part One: Yet Another Dragnet Surveillance Capitalist Cautionary Tale

September 2017

Authored by: James Scott, Sr. Fellow, ICIT

Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Support ICIT

Information should be liberated, not commoditized.

This powerful philosophy is the bedrock of the Institute for Critical Infrastructure Technology (ICIT), a nonprofit, nonpartisan 501(c)(3) cybersecurity think tank located in Washington, D.C. Through objective research, publications and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark.

Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/

Contents

Abstract 5
Equifax Is Yet Another Negligent Data Broker 5
What is Equifax? 7
Who was Securing Equifax Customer Data? 8
David Webb, Equifax CIO, Linguistic Business Administrator 8
Susan Mauldin, Equifax CSO, Musical Composer 8
Reliance on Unqualified Equifax Executives Invited Breaches 9
Details of the Equifax Breach 10
Low-Level Attackers are Using Equifax as a Claim to Fame 11
"They quite frankly didn't know what they were doing." 15
Equifax's Disastrous Incident Response 15
Three Executives Dumping Stock Appears More Conspiracy than Coincidence 15
Equifax Practically Launched its Own Phishing Site 15
Equifax Baits Victims with Free Credit Monitoring and Later Switches the Details 16
Terms and Conditions Apply to Equifax Incident Response 17
Consumer Actions 18
Enroll in Free Credit Monitoring 18
Freeze Your Credit 19
Place a Fraud Alert 19
Monitor Accounts 19
Manage Credit Cards 19
Beware Predatory Vendors and Faux Experts 19
Remain Vigilant Against Malicious Campaigns 20
Legal Action 20
Experian and TransUnion May Also be Compromised 21
Organizational Remediation 23
Non-Technical Controls 23
Develop an Information Security Team 23
Heed the Information Security Team 24

Protect Data According to its Value 24
Update and Patch Systems 24
The Principle of Least Privilege 24
Limit Access to Necessity 24
Segregate Administrative Duties Based on Role 25
Technical Controls 25
Data Encryption 25
Data Loss Prevention (DLP): 25
Network Segmentation 26
System Information and Event Management (SIEM) 26
Machine Learning-Based Artificial Intelligence Solutions 27
User and Entity Behavioral Analytics (UEBA) 27
Identity and Access Management (IAM) 27
Conclusion 28
Sources 30

Abstract

A catastrophic breach of Equifax's systems was inevitable because of systemic organizational disregard for cybersecurity and cyber-hygiene best practices, as well as Equifax's reliance on unqualified executives for information security. On September 7, 2017, Equifax publicly disclosed that a remote adversary had exfiltrated an estimated 143 million U.S. credit records over the course of a two-month period. Equifax knowingly waited six weeks to inform 44 percent of the American population that their credit records were compromised by an unknown adversary who exploited the negligently unpatched Apache Struts (CVE-2017-5638) vulnerability, despite the company's ability to mitigate the vulnerability two months prior to the compromise. Meanwhile, Equifax executives dumped their stock, removed key language from its terms and conditions, and its executives planned numerous attempts to leverage incident response and remediation against the victims who never knowingly permitted Equifax to aggregate and disseminate their data in the first place. Equifax has proven itself to be a compromised, irresponsible data custodian; however, Experian and TransUnion may be just as vulnerable, irresponsible, and compromised. Significant technical and non-technical cybersecurity and cyber-hygiene reform is necessary to protect consumers from the lackadaisical practices of under-regulated data brokers.

Equifax Is Yet Another Negligent Data Broker

Data brokers continue to jeopardize the long-term safety and security of the consumers who are trapped in their dragnet surveillance and incessantly manipulated by their demographic and psychographic Big Data algorithms. To them, information is a commodity and people are seen as data points instead of human beings. Data brokers continue to practice lackadaisical cybersecurity because they fail to connect the information lost in countless breaches to the lives impacted by adversaries' campaigns. Equifax is yet another negligent data broker that has been compromised due to its failure to secure data according to its value, promote cyber-hygiene best practices, and implement layered defenses. Despite jeopardizing the Social Security numbers and other sensitive information of 44 percent of the U.S. population, it is unlikely that Equifax will be the last data broker compromised before the public and private sector collaborate on meaningful reform. It may not even be the last compromised this year. Based on early 2017 monitoring of now-defunct Deep Web markets, Experian and TransUnion might be likewise compromised. The public should have no confidence whatsoever in the companies collecting, storing, transmitting, or processing their metadata (often without their knowledge, awareness, or consent). ISPs, data brokers, and similar organizations have a long and sustained history of operating insecurely and shifting risk to consumers instead of protecting their data. Data from ISP systems are already available on Deep Web markets and forums. Furthermore, insufficient regulations and consumer protections are implemented to secure customers from the emerging threat. Users often cannot change their ISPs and do not know which companies are exchanging or exploiting their data. In effect, S.J. Res. 34 and other dragnet surveillance bills are ensuring that consumers are exploited without their knowledge, awareness, or consent and that the

organizations mishandling the data and failing to secure their systems are not held accountable in any meaningful way. Data must be protected according to its value and potential uses, whenever it is collected, wherever it is stored, whenever it is processed, and however it is transmitted. Risks of unsolicited exposure, disclosure, or compromise are best reduced by limiting the parties with access to the data and considering emerging exploitation vectors when deciding whether to collect, store, or transmit information. Populations will suffer from improper data handling, and the effects will eventually create a backlash for public and private businesses and legislators.

Figure 1: Dumped Equifax Credit Reports

Figure 1 depicts an AlphaBay listing captured on January 18, 2017, that full Equifax reports were dumped from the Equifax API. This could indicate that Equifax was breached by multiple attackers concurrently or in multiple events.

Credit history and eligibility in the United States is monitored and reported by three bureaus – Equifax, TransUnion, and Experian. These three bureaus govern some of the most pivotal decisions of consumers' lives, yet very little is done to ensure that they are handling the data that they store, process, or transmit responsibly. In fact, as private companies, the bureaus are not subject to some of the more stringent cybersecurity and cyber-hygiene requirements applied to federal critical infrastructure systems. Furthermore, the bureaus lack access to the bleeding-edge

layered defense-grade solutions necessary to repel the malicious campaigns of sophisticated cyber-mercenaries and nation-state sponsored Advanced Persistent Threats (APTs).

Consumers do not have the ability to decide whether these data brokers collect information about them in massive capitalist dragnet surveillance. The collected PII, psychographic, and demographic data, whether correct or false, is deterministic in decisions that directly influence the wealth and well-being of consumers via loan applications, some employment decisions, and other key decisions. Equifax, a major data broker, negligently handled consumer data, and as a result, unknown adversaries now possess the credit information of nearly half of the U.S. population. On September 7, 2017, Equifax revealed to the public that months prior it had been the victim of one of the largest cyberattacks in U.S. history. Personal Identifiable Information (PII) corresponding to 143 million citizens – 44 percent of the population – was exfiltrated by an unidentified adversary due to Equifax's lax cybersecurity controls and cyber-hygiene practices. PII included names, Social Security numbers, birthdates and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also exposed. Worse, for over five weeks, Equifax intentionally delayed notifying consumers of the compromise and potential malicious exchange and exploitation of their data. Consumers cannot opt out of the bureau's reporting of their "credit score."

The lackadaisical cybersecurity and cyber-hygiene of data brokers is neither novel nor surprising. In numerous past blog posts and whitepapers, ICIT has reported on the willful negligence of data brokers and the lack of governance and oversight pertaining to their activities. There is a strong likelihood that a malicious adversary that compromised Equifax's network long enough to exfiltrate 143 million citizen profiles also laterally compromised associated networks and systems. There is a reasonable likelihood that a forensic analysis of networks belonging to Experian and TransUnion will reveal compromise by the same adversary or different threat actors using the same tools, techniques and procedures [1]. Screen captures of Deep Web listings gathered in early 2017 may indicate that Experian and TransUnion are likewise compromised, albeit not to the same degree.

What is Equifax?

Equifax is one of the largest consumer credit reporting agencies, allegedly possessing data on approximately 800 million consumers and 90 million businesses. Equifax is a major data broker. Through services such as credit monitoring, it generates annual revenue exceeding $3 billion. Equifax, along with Experian and TransUnion, collects demographic and psychographic data points from smaller data brokers that monitor financial transactions and other behavior indicators. Aggregated information is leveraged in complex proprietary algorithms to assign each consumer a credit score that is meant to inform lenders' decisions on whether to lend to the applicant based on their historical and forecasted fiscal risk. In a broad sense, Equifax, Experian, and TransUnion impact the decision behind every application for a loan, credit card, or mortgage.

Who was Securing Equifax Customer Data?

Following the breach, Equifax announced that the chief information officer and chief security officer would be "retiring early." To evaluate the systemic un-cyber-hygienic culture permeating Equifax, it is worth understanding that these individuals were previously tasked with securing consumers' information. This discussion is not meant to "dox" these individuals. Given that their "retirements" have already been announced and media attention has already followed, this report will focus on Equifax's information security culture.

David Webb, Equifax CIO, Linguistic Business Administrator

From 2010 until the time of the breach, Equifax's CIO was David Webb, who was responsible for "leading a global team of IT professionals in delivering the technology strategy as well as support for the company's innovative consumer and business solutions." Webb had previously worked as a senior executive in IT operations and financial services in organizations such as Silicon Valley Bank, Goldman Sachs, Bank One, and GE Capital's auto finance business. He also held advisory positions at Kestrel Data, Marathon Oil UK, and Brown & Root. He earned a bachelor's degree in Russian from the University of London and a master's degree in business administration from the J.L. Kellogg Graduate School of Management at Northwestern University. In a September 2016 Silicon Republic interview, Webb repeatedly stressed that his goal was to increase revenue and grow Equifax's business. He never mentioned security as a priority or a necessary duty of his position [2].

Susan Mauldin, Equifax CSO, Musical Composer

Equifax's CSO was Susan Mauldin. Although she did have 14 years of private sector experience, Mauldin's educational background in music composition likely did not prepare her to secure over 800 million credit records. Since disclosure of the breach, Equifax has attempted to distance itself from Mauldin by deleting two video interviews, removing a podcast, removing her profile from the website (while David Webb remains), and changing her last name on LinkedIn to "M." before removing her profile altogether.

Figure 2: Susan Mauldin, Equifax's Resident Composer

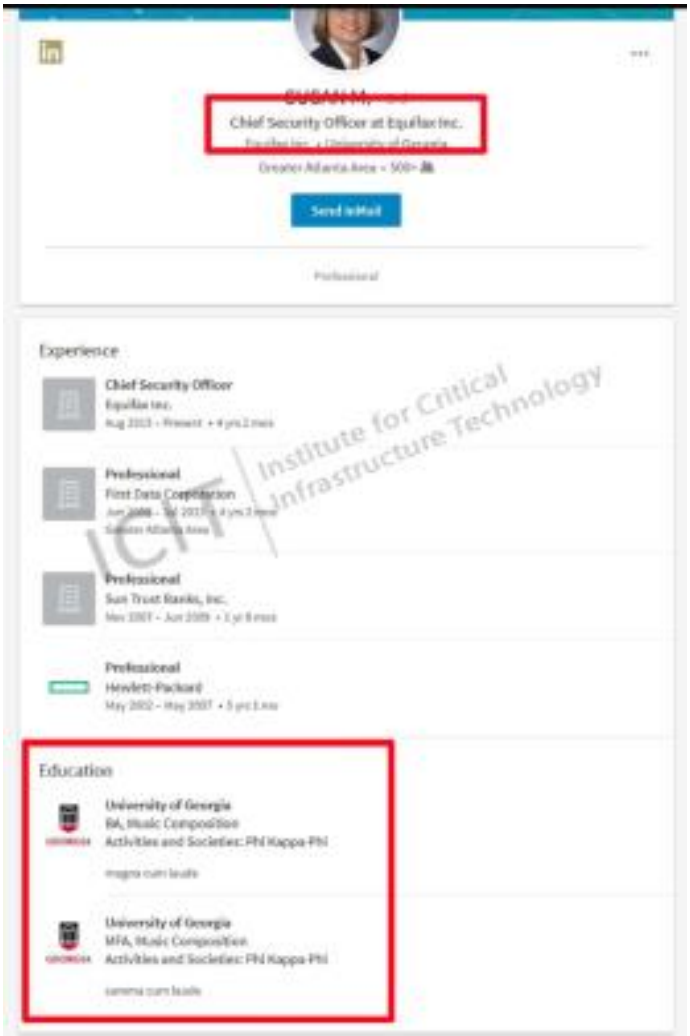


Figure 2 features the now removed LinkedIn page of Equifax CSO Susan Mauldin, who "retired early." As CSO, she was responsible for securing Equifax systems, including the servers that were breached due to Equifax's failure to apply the patch that mitigated CVE-2017-5638. Neither CSO Susan Mauldin nor CIO David Webb were formally trained in information security.

Reliance on Unqualified Equifax Executives Invited Breaches

A breach of Equifax systems was inevitable. Neither of the executives charged with securing millions of data records had the qualifications or background necessary to complete their tasks. In the cases of Webb and Mauldin, Equifax senior management should not have hired personnel without information security training to manage highly sensitive systems and data. Even if CVE-2017-5638 were patched, attackers likely would have found a vector to compromise Equifax's systems because the C-suite exhibited systemic negligence, a lack of cyber-hygiene, and a disregard for information security training and qualified personnel. If CEO Richard Smith eventually faces a Congressional inquiry, he may need to justify why he felt comfortable

entrusting the security of millions of highly sensitive consumer records to two individuals without any qualifications to secure those records [3]. Russ Ayres has been appointed interim CSO, and Mark Rohrwasser was named interim CIO. Ayres is the former vice president of Equifax's IT unit, while Rohrwasser previously led Equifax's international IT operations [4].

Details of the Equifax Breach

On September 7, 2017, Equifax announced that between mid-May and late July 2017, remote adversaries compromised its systems and exfiltrated 143 million credit records of U.S. consumers and more than 400,000 records of U.K. and Canadian consumers. The bureau also reported the unauthorized disclosure of 209,000 U.S. credit card numbers and 189,000 dispute records containing personally identifying information. This amounts to nearly a quarter of Equifax's treasure trove of PII and credit card information that it accumulated via dragnet surveillance; its offered services; and exchanges with third-party data brokers, such as credit card companies and financial institutions. Roughly 44 percent of the United States population is known to be compromised, but ongoing forensic analysis of the breach could reveal that significantly more records were exfiltrated. The vast majority of impacted consumers were not willing customers of Equifax. They never gave permission for Equifax, Experian, or TransUnion to aggregate their data from services and financial product providers or to redistribute that data to additional third parties. Victims were never offered informed notice or choice concerning the collection, application, or exchange of their information [5].

Six days after the incident was disclosed, Equifax released high-level details of the incident in response to public outcry and pressure from a bipartisan group of U.S. senators. Remote adversaries compromised Equifax systems by leveraging an Apache Strut exploit (CVE-2017-5638). A patch mitigating the vulnerability was released in March 2017 – two months prior to the compromise – but Equifax neglected to update and patch its systems in a timely manner. In all fairness, it is nearly impossible to anticipate which vulnerabilities attackers will exploit. A seemingly minor flaw could facilitate massive attacks if left unremediated. As a best practice, organizations should ensure that patches and updates are applied as soon as possible after release. Given that the vulnerability remained unpatched in late July, months after the release, it appears that Equifax lacked any cyber-hygienic initiative to adhere to best practices [5].

On September 12, 2017, researchers at Hold Security LLC discovered that the Veraz online portal, designed to authenticate Argentinian Equifax personnel, was vulnerable to remote adversarial compromise using the default credentials "admin / admin." Inside the portal, researchers were able to view the names, email addresses, and employee IDs of more than 100 Equifax employees in Argentina. Equifax has an estimated 111 employees in Argentina. A clickable button enabled the authenticated administrator to add, modify, or delete accounts. Employee records included a plaintext username and an obfuscated password, which could be easily discovered in the "view source" panel of the HTML code. All employee passwords were discovered to be the same as that user's username, which consisted of their last name or a

combination of their first initial and last name. Given that most of the personnel are visible on LinkedIn, any remote attacker could have easily accessed the credit dispute portal. The portal contained 14,000 records (715 pages) that represented a decade's worth of fax, email, and phone complaints and disputes. Each customer's DNI (the Argentinian equivalent of a Social Security number) was listed next to the case file. Following public disclosure, Equifax has disabled the Veraz portal pending an investigation. Equifax also operates in Brazil, Chile, Ecuador, Paraguay, Peru, and Uruguay, and it remains unclear if similar flaws are present in web portals oriented toward those sites [6].

Low-Level Attackers are Using Equifax as a Claim to Fame

A host of scam artists and unsophisticated script kiddies have already attempted to claim responsibility for the Equifax breach or to market data allegedly exfiltrated from Equifax's servers. One actor demanded that a ransom of 600 Bitcoins be paid before September 15, 2017, or else the entire treasure trove of exfiltrated data would be publicly released. Security researchers discovered a misconfiguration of the services site, identified its hosting service, and quickly shut the site down [7] [8].

Figure 3: The "Equihax" Onion Site

The "Equihax" threat actors claim responsibility for the breach. Though they claim to be interested solely in impacting Equifax, the group has listed Bitcoin costs for exfiltrated data (allegedly as an ironic joke). The veracity of their claim is contested at the time of this writing because of a lack of definitive proof. If true, however, the group's claim that they "have had access for years now" merits further investigation.

Another collection of actors, the self-named "Equihax" group, recently conducted an interview in which they claim responsibility for the attack and detail the tools, tactics, procedures, and methodologies used. "Equihax" appears to be hacktivists turned cybercriminals. The group provided screenshots of insecure management panels, including an Equifax instance of IBM WebSphere, which the group's actors allegedly compromised in the attack [9] [8]. Security researchers confirmed in the days following the breach that Equifax was using WebSphere to

power its public-facing website [7]. The interviewer alleges that the panels were discoverable using the Shodan IoT search engine prior to Equifax's public disclosure of the breach. The hacker stated, "If I have to release the information and make it public for these companies to finally acknowledge and admit their fuck ups (maybe not blame on apache flaw either) then I will." The threat actor created a Deep Web site offering the records in exchange for Bitcoins. In the interview, however, the group admitted that the Bitcoin component was only added to garner more media attention and to mock fake sellers and that the campaign was never meant to capitalize on the exfiltrated data. The "Equihax" actors allegedly had access to Equifax subdomain panels, governing credit reports, analytics, switchboards and other functions. The hackers claim that while the panels were encrypted, the private keys were embedded in the panels themselves. The interviewer claims to have verified that data using Equifax's TrustedID Premier tool [9].

Figure 4: "Equihax" Donald Trump Sample

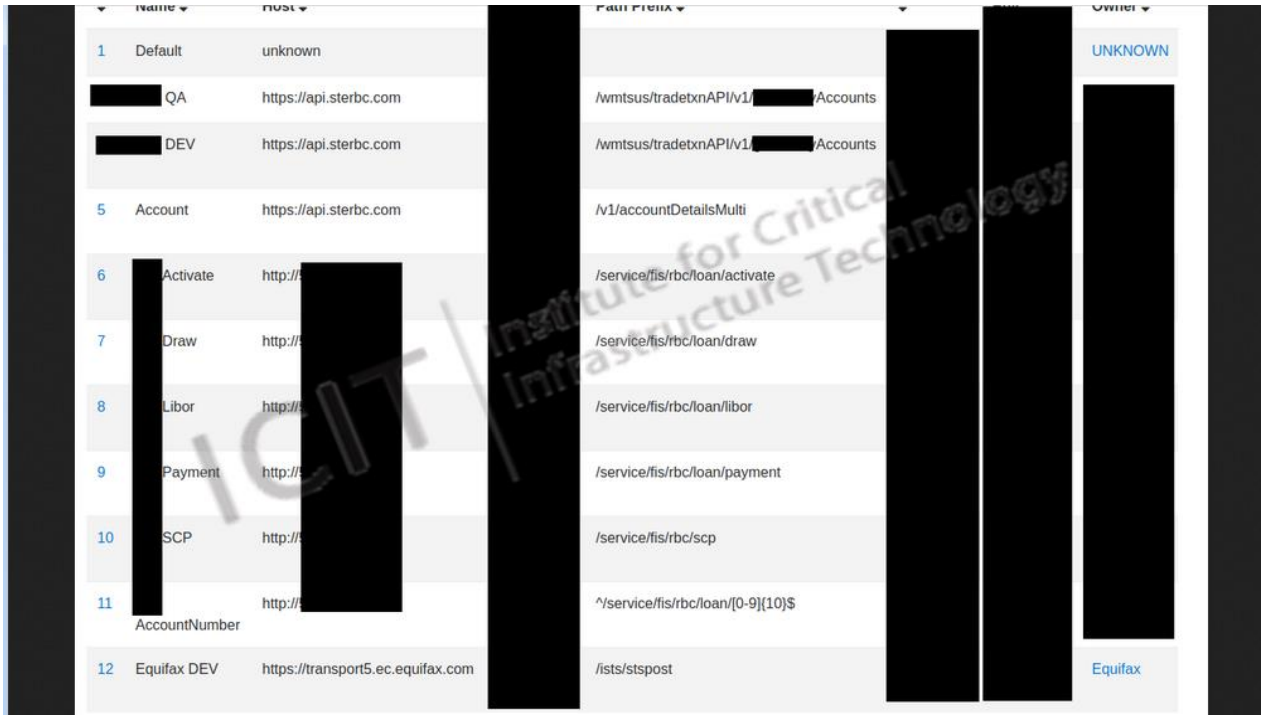

```
{
  "requestId" : null,
  "ssn" : "086385955",
  "dob" : "06/14/1946",
  "firstName" : "DONALD",
  "lastName" : "TRUMP",
  "middleName" : "JOHN",
  "city" : "NEW YORK",
  "state" : "NY",
  "streetName" : "5TH",
  "streetType" : "AVE",
  "streetNumber" : "725",
  "postalCode" : "10022",
  "fraudCode" : null,
  "fraudMessage" : null,
  "totalLiability" : null,
  "equifaxStatus" : null,
  "creditScore" : 819,
  "creditReportResourceId" : 2389,
  "creditReportFileSize" : null,
  "creditReportName" : "data/equifax/20170520/1d6c7cd0-a41d-ed29-4b19-b8394fa87d59.pdf",
  "creditReportMimeType" : "pdf",
  "creditReportSha1CheckSum" : "85b1ab26e5b2d45805a5daaf78d5d6c234300c61",
  "errorCode" : 0,
  "errorMessage" : null,
  "equifaxErrorInfo" : null,
  "createdTime" : "2017-05-20T12:19:12.000+0000",
  "updatedTime" : "2017-05-20T14:39:36.000+0000",
```


ICIT Institute for Critical Infrastructure Technology

In an attempt to prove that they compromised Equifax, the self-proclaimed "Equihax" group provided a JSON record of information allegedly belonging to Donald Trump. Some security researchers contend that Trump's information has been available for years and that the format of the data does not correspond to Equifax systems [8].

The “Equihax” claim could be legitimate, or it may be yet another fabrication meant to garner fame and Bitcoins. The screenshots provided contain too much redacted information to verify the claims of the hackers. Furthermore, the provided images appear “spares” and “corporate,” but some security researchers allege that they are nothing but dubious constructs. Of note, the applications listed, such as the interbank loan system Libor (the London Interbank Offered Rate), and captured URLs could indicate that the screen captures are from a different network, such as the Royal Bank of Canada. Information in the sample data profiles of Donald Trump and Kim Kardashian have allegedly been disclosed before. Finally, the sample data was presented as a text file and formatted in JSON (JavaScript Object Notation). After posting the listing, Twitter users commented on an error in the state listed on a sample of Bill Gates’ data. The sample was later changed to fix the typographical error. The bottom line is that while it is possible that the “Equihax” group was behind the Equifax breach, it is equally likely, if not more so, that a still obfuscated adversary exfiltrated the data and is biding its time until the data can be leveraged in additional attacks or sold on Deep Web markets without drawing the full ire of the U.S. intelligence and information security communities [8].

Figure 5: Redacted “Equihax” Sample



	Name	Host	Path Prefix	Owner
1	Default	unknown		UNKNOWN
[redacted]	QA	https://api.sterbc.com	/wmtsus/tradetxnAPI/v1/[redacted]/Accounts	[redacted]
[redacted]	DEV	https://api.sterbc.com	/wmtsus/tradetxnAPI/v1/[redacted]/Accounts	
5	Account	https://api.sterbc.com	/v1/accountDetailsMulti	
6	[redacted] Activate	http://[redacted]	/service/fis/rbc/loan/activate	
7	Draw	http://[redacted]	/service/fis/rbc/loan/draw	
8	Libor	http://[redacted]	/service/fis/rbc/loan/libor	
9	Payment	http://[redacted]	/service/fis/rbc/loan/payment	
10	SCP	http://[redacted]	/service/fis/rbc/scp	
11	[redacted] AccountNumber	http://[redacted]	^/service/fis/rbc/loan/[0-9]{10}$	
12	Equifax DEV	https://transport5.ec.equifax.com	/ists/stspost	Equifax

The “Equihax” group provided heavily redacted samples on its onion site as “proof” that it comprised Equifax. Not enough information remains for security researchers to verify the threat actor’s claim. Consequently, some see the redactions as evidence that “Equihax” is yet another scam.

"They quite frankly didn't know what they were doing."

Equifax removed its mobile applications from the Apple store and Google Play at roughly the same time it announced the breach. Though there is no indication that the apps were associated with the incident, they reportedly suffered from numerous vulnerabilities that allowed for man-in-the-middle and other attacks because some components relied on HTTP rather than HTTPS [10]. As a result, in the locations that used HTTP, data communicated between users and Equifax were not encrypted. Security researcher Jerry Decime, who discovered the vulnerability, argues, "They quite frankly didn't know what they were doing." As a best practice, all mobile applications, especially those that ask for sensitive information, should rely on HTTPS [10].

Equifax's Disastrous Incident Response

It is difficult to imagine how Equifax could have managed the public disclosure and incident response more tumultuously following the compromise of sensitive information of nearly half the populations of the United States and the United Kingdom (for whom incident response instructions still have not been issued at the time of this writing). Equifax delayed publicly disclosing the breach to consumers for nearly six months; likely in an attempt to manage negative public response, mitigate reputational harm, and pre-empt litigation.

Three Executives Dumping Stock Appears More Conspiracy than Coincidence

Two days after the discovery of the breach and more than a month prior to public disclosure, three Equifax senior executives, including the chief financial officer, sold stock amounting to an estimated $1.78 million. The Equifax executives contend that the sale was coincidental [11]. One executive selling stock around the time of discovery of a major breach could be a coincidence. Two executives selling stock before revealing catastrophic organization-wide negligence appears to be collusion, but it could still be happenstance. Three executives selling millions of stock prior to disclosing severe mismanagement of consumer data publicly, which resulted in a 30 percent fall in stock price, merits investigation. If the senior executives had prior knowledge of the incident, then they are in contravention of insider trading laws. A bipartisan group of 36 senators agrees and subsequently sent a letter to the Security and Exchange Commission, Department of Justice, and Federal Trade Commission. At the time of this writing, the FTC has confirmed that it will investigate the stock sales following the breach [5].

Equifax Practically Launched its Own Phishing Site

As part of its incident remediation campaign, Equifax set up equifaxsecurity2017.com for consumers to check whether they have been affected by the breach and to sign up for a free year of the TrustedID credit monitoring service. Since adults in the United States have nearly a 50/50 chance of having their information compromised by the Equifax breach, the website frequently collapsed under the volume of visitor traffic in the week following Equifax's announcement and has only been intermittently functional. Furthermore, since the initial breach may have been

facilitated by a vulnerability in a web interface, users visiting the site should be concerned about the underlying security. Other cybercriminals and script kiddie attackers may attempt to compromise the remediation web portal to collect input data or to leverage it as a watering-hole site. Alternately, attackers may attempt to lure users to spoofed sites or malicious landing pages bearing similar names. This task may be easier than expected, since the oddly titled "equifaxsecurity2017" already resembles a phishing site in name and features an abundance of characters that adversaries can easily substitute when constructing malicious landing pages. In fact, for days following the disclosure of the breach, OpenDNS and some browsers blocked Equifax's consumer incident response portal because the domain name algorithmically matched that of watering-hole sites [5] [11]. To limit potential scams, security firm Mandiant – which was hired to investigate the incident – has been purchasing domains since September 5, 2017, that could be leveraged in phishing campaigns [11].

Those who actually visited the victim portal could enter their name and six digits of their Social Security number to determine whether their information was compromised. Within hours of the launch of the site, reports circulated that the interface was unreliable. Multiple entries of the same data yielded differing answers as to whether the consumer's information was compromised. Furthermore, some users claim that the entry of false information or the combination of legitimate and false data (such as a fake name and real SSN) defaulted to a confirmation that the user was compromised. For the sake of security and immediate action, rather than rely on a poorly designed and possibly insecure tool, consumers should assume themselves compromised and follow the recommended victim response best practices detailed later [5].

Equifax Baits Victims with Free Credit Monitoring and Later Switches the Details

Those users brave enough to enter their sensitive data into Equifax's hastily constructed tool and lucky enough for it to remain stable long enough to confirm their status may have been welcomed by a vague statement about the breach and an encouragement to enroll in Equifax's TrustedID Premier service. The bureau did not recognize any conflict or guilt in asking potential fraud victims of the breach caused by Equifax's negligence to enroll in the fraud protection service owned and operated by Equifax [5]. Immediately following the incident, it appeared to victims that registering for Equifax's credit monitoring service, through TrustedID, would waive their right to join a class-action lawsuit against the bureau; however, after viral social media attention and public outrage, Equifax updated its site to clarify that the terms of service of the Equifax site and the TrustedID service do not apply to this data breach. The underhanded attempt to exploit the engineered ignorance of guiltless victims of the incident further by hiding vital details within lengthy and predominantly ignored terms of service agreements demonstrates Equifax's lack of remorse and integrity. If consumers had not leveraged negative media attention against the organization, Equifax likely would not have rescinded or "clarified" its position on offered mitigation services, which it is compelled to offer. Offering a free year of credit monitoring is not a philanthropic gesture; Equifax owns TrustedID. While Equifax clarified that

victims who sign up for the service will not waive their rights to join class-action lawsuits, it did not waive the clauses pertaining to TrustedID's automatic renewal. Any citizen who does not call the company to cancel the service after the "free year" will be billed. Considering that many consumers would like to monitor their credit for more than a year given attackers' ability to exploit the stolen PII for decades, Equifax is essentially leveraging the fear of victims to increase the long-term clients of its monetized services, likely so that it can use the funds to repair its crumbling reputation and status. It also needs the capital to pay fines and fight legal battles since its insurance may be insufficient to cover the costs associated with the incident [1].

In any incident that necessitates ineffectual credit monitoring, most Information Security professionals recommend that victims freeze their credit instead. Credit freezes prevent criminals from exploiting stolen information along with a majority, but not all, of attack vectors, while credit monitoring just informs the client of potential exploitation after it occurs. Consumer credit is frozen separately by Equifax, Experian, and TransUnion. Enrollment in TrustedID enabled victims to freeze their credit through Equifax. The firm requires users to input a 10-digit PIN to request account unlocks. Normally, a lengthy code would be computationally resource-intensive to break, but until yet another wave of consumer backlash, Equifax auto-generated PINs that corresponded to the data and time of the requested removal. For example, a unfreeze request of September 11, 2017, at 10 a.m. would simply be 0911171000. This level of "security" is laughable, considering that reliable random number generators are readily available from an overwhelming plethora of sources [1] [12]. In response to overwhelming public condemnation, Equifax subsequently announced that it would soon transition to a new PIN generation system and that consumers could request more secure PINs be sent to their registered mailing address [5].

Terms and Conditions Apply to Equifax Incident Response

Equifax spent nearly six weeks intentionally keeping consumers unaware of the bureau's failings. That time was not used to analyze the network forensically and provide a public, holistic report of the breach, or to develop a comprehensive plan to ensure that the compromised data was not weaponized against consumers by malicious cybercriminals, digital mercenaries, or other threat actors. Equifax delayed releasing details of the breach publicly because the organization, which admonishes consumers for "irresponsible choices" and has the power to report (potentially incorrect) information that determines life-altering financial decisions based on "responsible actions," was itself wholly and egregiously irresponsible with the consumer data that it collected through solicited and unsolicited dragnet surveillance. Between discovery of the compromise in late July and disclosure in early September, Equifax heavily revised its terms of service, reducing it from 7,202 words to 2,869 words. Removed sections include:

- Notification that its monitoring services does not and will not improve consumer credit.

- Notification that its services would not place a fraud alert with consumer reporting agencies
- Information regarding how Equifax derives its credit scores from its own internal formula, and that credit scores do not correspond to the ratings used by banks and other financial institutions
- Information about service billing, except clauses concerning automatically renewing memberships
- Details about offered identity theft products, including their limitations, capabilities, and how they operate
- Details on how Equifax manages disputes and calculates liability and warranty coverage

Equifax did not remove two-thirds of its terms of service because it feared that consumers would be overwhelmed by the language or confused by the applications. It did not remove the details out of fear that victims might inflate the protective capabilities of offered mitigation and remediation services. It eliminated vital details in a self-serving attempt to limit potential lawsuits and distract from the limitations of its products and their lack of necessity to the public [1].

Consumer Actions

Since forensic analysis of Equifax systems is ongoing and the incident response tools provided by Equifax are unreliable, consumers should assume their information compromised unless later proven otherwise. The credit and PII exfiltrated in the breach will retain value for years or decades. The Equifax breach, along with OPM, Anthem, and countless others in recent years, may finally force user authentication by means other than PII. Qualifiers such as Social Security numbers were introduced as a means of identification, not authentication. If SSN, birth date, mother's maiden name, and other personally identifying information were phased out as authenticators, then the information exfiltrated in innumerable breaches would rapidly devalue. Until then, consumers can take the following actions to limit the impact of the Equifax breach.

Enroll in Free Credit Monitoring

Credit monitoring services alert the customer to changes in their credit score, new accounts, large transactions, and other suspicious account activity that could impact their financial stability negatively. The services are retroactive and require the alerted user to dispute any nefarious activity. Credit monitoring services rarely prevent identity theft; but, they alert the subject to potential compromise, and they do not require constant attention like credit freezes might. Free and low-cost monitoring is available to those users still comfortable entrusting their data to Equifax and other data brokers. Equifax's TrustedID, Symantec's Lifelock, and Credit Karma are all ID monitoring services marketed toward consumers. While some services or portions of

services might be free, users should read the terms and conditions and be wary of fiscal commitments [13].

Freeze Your Credit

Credit freezes prevent potential creditors or anyone else from viewing or modifying the subject's credit history or files until they issue a temporary or permanent "thaw" using a secure PIN. Freezes restrict the impact of identity theft by preventing the establishment of new accounts. Freezes usually cost a small fee to implement or remove, and some last for a set period. Equifax is offering free credit freezes for the weeks following the disclosure of the breach. Interested readers can request a freeze from each bureau online or via [13]:

- Equifax: 1-800-349-9960
- Experian: 1‑888‑397‑3742
- TransUnion: 1-888-909-8872

Place a Fraud Alert

A fraud alert is a less restrictive, but less secure, alternative to a credit freeze. Consumers can set fraud alerts at any one of the three major credit bureaus. After an alert is placed, potential creditors will be asked to verify their identity before issuing credit in their name [13].

Monitor Accounts

Consumers should incorporate the monitoring of any potentially compromised accounts into their daily routine. Account passwords should be complex, distinct, and regularly updated. Some users may find that password manager applications are necessary to improve their cyber-hygiene. Multi-factor authentication should be enabled whenever possible. A free annual credit report can be obtained from each bureau at AnnualCreditReport.com. The report will reveal any new accounts, any credit inquiries that occurred when the consumer did not apply for credit, and any balances that do not match the received statements [13] [14].

Manage Credit Cards

Potential victims should request new cards and account numbers from credit institutions. Text and email alerts can be used to monitor purchases actively. Monitoring credit card statements is especially important, because attackers often "test" victims by making a small innocuous purchase and monitoring whether the cardholder notices. Those who do not are prime targets for exploitation [13] [14].

Beware Predatory Vendors and Faux Experts

If a vendor was to inflate the price of necessary commodities to disaster victims, the public, the media, and potentially lawmakers would condemn or reprimand that organization. The same rule does not apply to breach victims. Vendors claiming panacea protections and silver-bullet solutions will target businesses that are worried about being similarly compromised. Faux experts and disreputable services will target individual consumers in attempts to capitalize off

their victimization. Even Equifax and other data brokers attempt to recoup long-term costs by acclimating consumers to a service or good and then leveraging that comfort for later profit.

Remain Vigilant Against Malicious Campaigns

Given the scope and the sensitive data exfiltrated from Equifax systems, adversaries will target fearful consumers and victims alike. Phishing scams and social engineering campaigns will attempt to trick users into disclosing financial information, visiting malicious landing pages, or opening nefarious attachments. Equifax, Experian, and TransUnion will never contact consumers directly. Any received correspondence or communication should be considered highly suspect.

Legal Action

The quickest way to elicit a company's response is to introduce a meaningful economic impact. Rather than wait for a legislative or goodwill-driven reformation, it might be easier and more expeditious to compel Equifax to improve its cybersecurity and cyber-hygiene best practices by besieging it in legal conflicts until it protects consumers' information adequately, according to the potential impact of the unauthorized disclosure of that data on the data subjects.

Immediately following public disclosure of Equifax's failure to secure data according to its value, consumers and watchdog organizations filed 23 class-action lawsuits in 14 states. One class-action lawsuit filed in Oregon seeks damages up to $7 billion, which would bankrupt Equifax while offering a mere $500 per victim. The sum may not be enough to compensate consumers for a lifetime subject to the risk of identity theft, nor would it be enough to cover the cost of a lifetime of credit monitoring and credit freezes, but it may be the example that data brokers and other private entities require to finally invest in modernized, layered defenses that protect consumer data against adversarial compromise [5]. On the other hand, class-action lawsuits may take the pressure off lawmakers, enrich law firms, and result in minuscule compensation or reformation that benefits average consumers [11].

Recognizing that Equifax operates in all 50 states and can be sued at the state level, college student Joshua Browder expanded the functionality of his DoNotPay bot, an application designed to help users fight parking tickets without paying for legal representation. The application now assists users with the paperwork necessary to sue Equifax for up to $25,000 (depending on the state) in small claims court. Plaintiffs would still be required to argue the case in court with or without the assistance of legal representation [5].

Experian and TransUnion May Also be Compromised

Figure 6: Experian May Also Be Compromised

Experian 203.419.083 entries complete dump Leaked database

USD 800.00
฿ 0.8901
In stock

Vendor doubleflag [+32|0] Level 8 (60+)
Class Digital
Delivery Instant Delivery

Quantity: 1
Buy Now
? Question
Report

hansamkt2rr6nfg3.onion

Listing Details

Experian complete dump 203.419.083
(THIS DATABASE NEVER BE A PART OF ALL LEAKED DATABASE PACKAGE)
have this field
FIELD DESCRIPTION
FIRST NAME
MI
LAST NAME
PREFIX
ADDRESS
SUITE/APT
CITY
STATE
ZIP5
ZIP4
DELIVERY POINT BAR CODE
FIPS STATE CODE
FIPS COUNTY CODE
LATITUDE
LONGITUDE
ADDRESS TYPE INDICATOR
0 = Undetermined
1 = Single Family Dwelling
2 = Apartment with unit designator
3 = Apartment without unit designator
4 = Rural Route
5 = Post Office Box
COMMUNITY REINVESTMENT ACT (CRA) INCOME CLASSIFICATION CODE
1 = LOW INCOME
2 = MODERATE INCOME
3 = MIDDLE INCOME

Figure 6 showcases a database dump sold on the Hansa Market prior to its shutdown on July 20, 2017, by Dutch authorities. Leaked Experian databases have appeared on Deep Web markets in the past and indicate that Experian may be as vulnerable as Equifax. Extensive forensic analysis, including penetration testing, of Experian and TransUnion networks is the only way to know if their systems are similarly compromised.

Equifax is not the first of the credit bureaus to experience a major security breach. Deep Web listings claiming to offer data exfiltrated from Equifax, Experian, and TransUnion typically appear annually between November and March, because the data is widely marketed to low-level scammers and script kiddies intent on committing tax fraud. In 2013, the United States Secret Service arrested Hieu Minh Ngo, the 24-year-old Vietnamese proprietor of the Superget[.]info Deep Web store. Ngo had gained access to the personal and financial records of over 200 million Americans by posing as a private investigator and paying for monthly access to Experian databases with wire transfers from Singapore. At the time of his arrest, he had been marketing over half a million "fullz" consisting of Social Security numbers, names, addresses, workplaces, mother's maiden names, email accounts, passwords, birthdates, driver's license records, and financial information. Furthermore, in October 2015, Experian disclosed compromise of the records of 15 million consumers who had applied for the "T-Mobile USA postpaid services or device financing from September 1, 2013, through September 16, 2015." Compromised information included names, addresses, Social Security Numbers, driver's license records, and passport numbers [11][15].

Figure 7: Alphabay Sale of TransUnion, Equifax, and Experian Reports

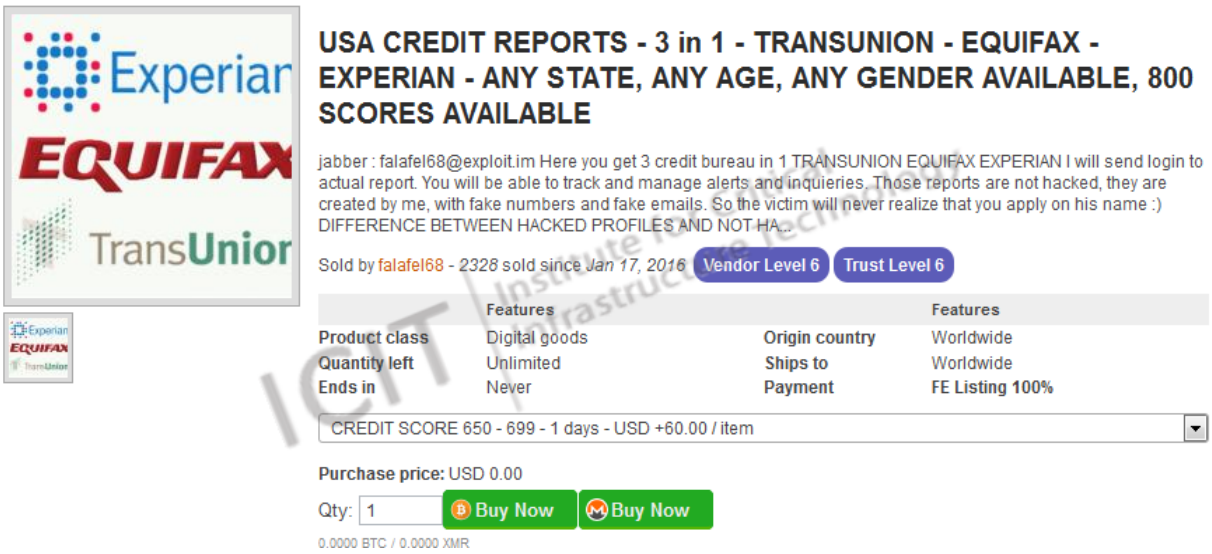


Figure 7 demonstrates that prior to the Equifax breach, attackers could retrieve and sell consumer credit reports. Attackers may have compromised a third party or spoofed a trusted affiliate network. In any case, data brokers, such as the credit bureaus, must improve their cybersecurity and cyber-hygiene to prevent adversaries from exfiltrating and exploiting consumer data.

Through periodic monitoring of the now-defunct Deep Web markets AlphaBay and Hansa Market in early January, ICIT captured a number of listings offering data allegedly obtained from Equifax, Experian, and TransUnion. While it is possible that numerous sellers inflated their source or that the data was obtained via the compromise of a third party, given the lackadaisical cybersecurity and cyber-hygiene practices of Equifax, it is equally possible that additional

attackers may have breached the data brokers' systems. AlphaBay and Hansa Market were both taken offline by an international law enforcement effort, and it is marginally possible that the FBI or Interpol captured data that could be used to track the sellers. In the meantime, comprehensive forensic analysis, complete with penetration testing, should be conducted on the networks of all three bureaus to ensure the safety and security of consumers.

Organizational Remediation

Equifax publicly stated that it plans to improve its cybersecurity posture and internal cyber-hygiene. Though the exact controls in place are not publicly disclosed, Equifax and similar organizations may consider the following recommendations in their attempt to improve security and implement comprehensive layered defenses systematically.

Non-Technical Controls

Cyber-hygiene and security-conscious corporate culture are as important as technical controls. The policies, procedures, practices, and guidelines ingrained in the organization define the parameters of its security posture.

Develop an Information Security Team

The data collected, stored, and transmitted by private sector data brokers, often without consumers' notice or choice, should not be managed by placeholder executives that lack a fundamental understanding of information security, cyber-security solutions, or organizational cyber-hygiene, such as the unqualified C-level management who recently "retired early" from Equifax. A qualified information security team with adequate resources is an organization's best defense against internal and external threats. The work of the information security team begins with a comprehensive risk analysis that identifies critical data assets; system vulnerabilities; risks according to the current threat landscape; and deficiencies in the organizational cybersecurity, cyber-hygiene training, or incident response plan. Without a risk assessment, the organization cannot make informed cybersecurity decisions.

It is often easier or more affordable to apply controls only to the most "important systems." The low-priority systems are often on the same network, but receive waivers and limited compensatory controls because of age, criticality to operations/mission, or availability and stability issues. Low-priority systems, such as web portals, often remain less secure than more significant assets such as financial systems; however, adversaries specifically target these vulnerable and often publicly discoverable systems to establish persistence, laterally compromise networked systems and exfiltrate data. If Equifax had controls in place to monitor data egress, it would have noticed the significant data traffic of 143 million consumers' information leaving its servers. Without qualified information security personnel, technical controls do little other than reinforce the C-suite's delusion of security. It is important that the C-suite and senior management consult the information security team on cybersecurity decisions, because the

executives may not grasp the realistic view of the organization's cyber-posture in relation to the modern threat landscape.

Heed the Information Security Team

In most incidents, the non-technical and technical controls implemented by the information security team as a result of a comprehensive risk assessment would have precluded the compromise of critical systems or the exfiltration of sensitive data if personnel had only acted in accordance with the implemented controls. All too often, the policies, procedures, guidelines, and controls implemented by the information security team are only paid lip service or are broadly interpreted. Admonitions urging employees to create complex passwords, recommendations to study policy documents, BYOD restrictions, and other conveyed information are often neglected by staff and upper management alike [16].

Protect Data According to its Value

Data brokers and other organizations in possession of treasure troves of sensitive PII, EHRs, and other valuable data are the constant targets of threat actors ranging from cybercriminals to nation-state sponsored APTs. The number or attempted and successful intrusions are limited when data is protected according to its value wherever it is stored, however it is transmitted, and whenever it is processed.

Update and Patch Systems

Systems and applications are investments that require the same level of due diligence and upkeep as tangible assets. Many organizations struggle with patch management, and there can be a significant gap between vulnerability revelation and system and application updates. That seems to have been the case with Equifax. Apache Struts (CVE-2017-5638) was made public on March 7, 2017, and a patch was made available on that very same day. To alleviate the burden of patching, organizations should automate patches wherever possible and incorporate regular updating and patching into the daily duties of a well-resourced information security team.

The Principle of Least Privilege

Critical assets may be servers containing personally identifiable information (PII), electronic health records (EHR), financial records, or intellectual property, or they could be vital services such as email, payroll, and networked device control panels. Personnel should only be assigned the least privileges necessary to fulfill their role in the organization. Privileges should be periodically reassessed to ensure that roles and needs have not changed, and to ensure that privileges are revoked from users who no longer perform the specified roles in the organization.

Limit Access to Necessity

Critical assets can be best protected by minimizing the number of people with access to only personnel who absolutely require access to fulfill their roles in the organization. Even if a position requires access to a critical asset, it may not require access to all the data contained within that asset.

Segregate Administrative Duties Based on Role

Administrative duties should be separated so that one individual does not have control over an entire process. For example, an employee should not be able to request, authorize, process, and receive payment for a product or service. No system administrator needs to have the highest level of permissions or carte blanche access to any data or system on the network. Segmenting administrative duties limits potential lateral movement.

Technical Controls

The financial sector may be the most ingrained and perseverant sector. Changes to critical systems and applications are often made over the course of decades, instead of months. Stagnant information security solutions can be a serious dilemma because antiquated legacy systems that rely on perimeter defenses are incapable of detecting, mitigating, or withstanding attacks from contemporary adversaries ranging from script kiddies to cybercriminals to APTs. Though defense-grade technical solutions remain available only to public sector critical infrastructure entities, private sector firms must invest in bleeding-edge systems, solutions, and services from repeatable vendors. At the time of this writing, it remains unclear what technical controls Equifax had implemented to protect its endpoints and exposed systems. Based on the current threat landscape, it should have implemented layered data-centric cybersecurity solutions that limited adversarial compromise, persistent presence, lateral movement, and data exfiltration and exploitation. Forensic analysis of Equifax systems will reveal whether they protected consumer data according to its value or whether they negligently declined investment in solutions and services to increase their profit margin at the expense of the safety and well-being of the consumers unwillingly caught in their surveillance dragnet.

Data Encryption

Data should be protected according to its value and the potential harm that would result if it were stolen. Encryption does not prevent adversaries or insiders from exfiltrating data; however, it does deter or prevent attackers from exploiting the stolen data unless they spend significant additional resources breaking the encryption or stealing the decryption keys. According to the "Equihax" attackers, Equifax did encrypt the data stored on their servers; however, the encryption keys necessary to decrypt and exploit the data were visibly stored as identifiers for each server.

Data Loss Prevention (DLP):

Data loss prevention is the employment of reliable vendor tools to secure data when it is in transit, when it is at rest, and when it resides at endpoints. DLP governs which data end users can transfer and which data can leave the network. DLP often includes keyboard filtering, USB port access control, network transfer monitoring, field-level encryption, and other mechanisms to deter internal and external threat actors [17] [18]. Equifax should have been suspicious of the amount of consumer traffic leaving its network, the prolonged activity of that traffic egress, and the external destination of millions of consumer data sets. If Equifax had invested in or licensed a DLP solution, automatic rules configured by a trained information security team would have

prevented any internal or external threats from exfiltrating sensitive consumer data from the network.

Network Segmentation

Network segmentation is the practice of dividing a network into smaller partitions, called subnets, to isolate critical assets from one another and control access to sensitive data. Networks can be logically segmented via private Virtual Local Area Networks (VLANs), which restrict communication between hosts on different subnets, in addition to being physically segregated via air-gaps. Logical segmentation involves the institution of conditional rules to determine which devices are allowed to communicate with one another. Various tools and systems are deployed to guard the gateway of each subnet, specifically to coordinate traffic flow, filter content, control access, and manage connections. Network segmentation prevents lateral compromise. If Equifax had properly segmented its network, then the attackers would not have been able to access consumer data via the public-facing web portal. Furthermore, data brokers such as Equifax should be legally mandated to segment servers containing consumer data so that a single adversary cannot exfiltrate millions of data sets.

System Information and Event Management (SIEM)

System Information and Event Management (SIEM) solutions are not foolproof, but they are a good starting point for incident detection and mitigation programs. SIEM solutions condense the event data from potentially thousands of devices and applications to a small number of actionable alerts that signal vulnerabilities, risks, and anomalous behavior that could be attributed to insider threats [19]. SIEM solutions provide a layered centric or heterogeneous holistic view into infrastructures, workflows, and compliance and log management in the form of dashboards or “views” [20]. Dashboard tools significantly reduce event response time and allow organizations to detect, prevent, and minimize the damage caused by an insider more effectively [21]. SIEM systems store, analyze, and correlate application security information and event data, such as authentication, anti-virus, audit and intrusion. [19]. These dashboards provide a streamlined and accelerated detection process by aggregating, prioritizing, and visualizing high-risk insider and cyber threat indicators from across all users, accounts, hosts, and enterprise endpoints [21]. Anomalous activities are detected by rules that alert the information security team of suspicious behaviors or fully automate responses based on predetermined conditions. SIEMs can be used to collect and centralize the event and log data across enterprise applications [19]. SIEM provides automated verification of continuous monitoring, trends, and auditing to show value to executives.

SIEM normalizes data as a two-part function that includes translating jargon to readable data to be displayed and visualized to user- or vendor-defined classifications and characterizations (field mapping). Data are given context and form relationships based on rules, architecture, and alerts to provide historical or real-time correlations [20]. SIEM alerts can be preconfigured with default/ prepackaged rules or customized to reflect the security policies and a profile of the

system under normal event conditions [19]. Finally, SIEMs are adaptable and scalable regardless of data source, application vendor, format, type, changes, or compliance requirements [20].

Machine Learning-Based Artificial Intelligence Solutions

Outdated insider threat protection paradigms are centered on the protection of endpoints. This model no longer reflects the modern threat landscape because adversaries have developed custom exploit kits and mutating malware that are not immediately detected by signature and heuristic-based anti-malware solutions. Machine-learning algorithms can process user and system activity data significantly faster than any human analyst. Consequently, algorithmic solutions can detect and mitigate malicious code and activity prior to adversarial execution. It can also prevent internal or external threats from escalating privileges, planting logic bombs, exploiting 0-days, or executing unwanted programs [22]. By securing the endpoint from malware, despite the lack of a signature or known malicious behavioral pattern, organizations prevent emerging threats from establishing persistence on the network, laterally compromising vulnerable systems, or exfiltrating treasure troves of sensitive user data.

User and Entity Behavioral Analytics (UEBA)

User and entity behavioral analytics (UEBA) solutions audit and analyze the file and application access of an individual to detect and connect disparate data points that could indicate suspicious user or application behavior. The information security team establishes a baseline of user activity (file access, logins, network activity, etc.) over a predetermined period of time and then uses that baseline to detect any time the user deviates from that norm and alert the information security team. UEBA solutions collect data from files, emails, IT resources, and other data streams without constraints on volume variety or velocity of data. In many cases, the solution is able to assess the data and generate alerts in near real-time [19]. UEBA excels at spotting variances in user and system activity and handling unknown instances. For example, UEBA can be used to detect automatically if a user deletes thousands of files in a short amount of time, starts visiting unusual directories or starts accessing applications that are not specific to their role, or if a server begins transferring millions of records that should not be leaving the network [19].

Identity and Access Management (IAM)

The Verizon 2016 Data Breach Investigations Report found that 63 percent of data breaches involved weak, default, or stolen credentials [23]. Effective cyber-hygiene hinges on each employee responsibly responding to every threat emerging from the hyper-evolving threat landscape. Personnel often find that cyber-hygiene is daunting, exhausting, and distracting; meanwhile, cybersecurity awareness and training are often limited, and the demanding responsibilities of personnel preclude their interest or ability to shore up their cyber-hygiene and their awareness of cybersecurity best practices [24]. Identity and access management (IAM) solutions centrally manage the provisioning and de-provisioning of identities, access, and privileges, and they manage the authentication and authorization of individual users within or across system and enterprise boundaries. IAM can automate the implementation of the principles of least privilege and least access across the network [25]. Privilege Identity Management (PIM)

solutions are a component of IAM through which user privileges and access rights are initiated at minimal values and readjusted when necessary according to the user's current role within the organization. PIM solutions enable the information security team to tailor access and privileges for internal personnel, outsourced/third-party users, and shared accounts across hybrid infrastructure. As a result, compromised credentials do not guarantee adversaries carte blanche access to sensitive servers and systems.

IAM solutions are critical to the protection of the identity perimeter across mobile and cloud infrastructures. Multi-factor authentication (MFA) can be used to validate user identities through a combination of user knowledge (such as a username, password, PIN, security question response, etc.); a user possession (such as a smartphone, smart card, token, one-time passcode, etc.); and information characteristic of the user (biometrics, retina scans, voice recognition, gait analysis, etc.) [24]. Multi-factor authentication would not have prevented the Equifax breach, but in the future, it can be implemented by Equifax and other organizations to limit the impact to victims by requiring an additional authentication component that is not based on PII or other compromised information.

Equifax has publicly claimed that it used tokenization to protect not only PCI data but also PII more broadly. If that's the case, given the size of the breach, it's unclear why so much data was exposed by the attack. Was there technology failure where the mapping table was exposed, or was there a failure in an Equifax process?

Conclusion

Equifax's inability to remediate the Apache Struts vulnerability with a readily available patch will cost the organizations millions or billions of dollars and will put nearly half of the United States population at risk of identity theft, fiscal fraud or medical account compromise for at least the next decade. Worse, because Equifax delayed disclosure and botched incident response, consumers are severely unprepared for the onslaught of social engineering campaigns and exploitative attacks that cybercriminals and techno-mercenaries are preparing to launch. The recommendations offered in this document can help consumers and organizations alike mitigate some of the emerging attack vectors and regain a semblance of control over their identity, sensitive information, and lives.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

[1] Hruska, J. (2017). *The Equifax Situation Continues to Worsen - ExtremeTech*. [online] ExtremeTech. Available at: https://www.extremetech.com/internet/255311-equifax-fine-print-keeps-getting-longer-situation-mostly-gets-worse [Accessed 18 Sep. 2017].

[2] Kennedy, J. (2017). *The five-minute CIO: Dave Webb, Equifax*. [online] Silicon Republic. Available at: https://www.siliconrepublic.com/enterprise/five-minute-cio-dave-webb-equifax [Accessed 18 Sep. 2017].

[3] Arends, B. (2017). *Equifax hired a music major as chief security officer and she has just retired*. [online] MarketWatch. Available at: http://www.marketwatch.com/story/equifax-ceo-hired-a-music-major-as-the-companys-chief-security-officer-2017-09-15 [Accessed 18 Sep. 2017].

[4] Surane, J. (2017). *Equifax Says CIO, Chief Security Officer to Exit After Hack*. [online] Bloomberg.com. Available at: https://www.bloomberg.com/news/articles/2017-09-15/equifax-says-cio-chief-security-officer-to-leave-after-breach [Accessed 18 Sep. 2017].

[5] Frew, J. (2017). *Equihax: One of the Most Calamitous Breaches of All Time*. [online] MakeUseOf. Available at: http://www.makeuseof.com/tag/equifax-breach-what-happened/ [Accessed 18 Sep. 2017].

[6] Krebs, B. (2017). *Ayuda! (Help!) Equifax Has My Data! — Krebs on Security*. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/ [Accessed 18 Sep. 2017].

[7] Weapons Grade Shinanigans. (2017). *[UPDATED] Finding the (Alleged) Equifax Hackers*. [online] Available at: https://wvualphasoldier.wordpress.com/2017/09/09/finding-the-alleged-equifax-hackers/amp/ [Accessed 18 Sep. 2017].

[8] Gallagher, S. (2017). *Scammers keep trying to sell fake Equifax facts*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2017/09/scammers-keep-trying-to-sell-fake-equifax-facts-asking/ [Accessed 18 Sep. 2017].

[9] Spuz.me. (2017). *SPUZ : Equifax Breached*. [online] Available at: http://spuz.me/blog/zine/3Qu1F4x.html [Accessed 18 Sep. 2017].

[10] Weissman, C. (2017). *Here's Why Equifax Yanked Its Apps From Apple And Google Last Week*. [online] Fast Company. Available at: https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week [Accessed 18 Sep. 2017].

[11] Krebs, B. (2017). *Equifax Breach Response Turns Dumpster Fire — Krebs on Security*. [online] Krebsonsecurity.com. Available at: https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/ [Accessed 18 Sep. 2017].

[12] Lieber, R. (2017). *After Equifax Breach, Here's Your Next Worry: Weak PINs*. [online] Nytimes.com. Available at: https://www.nytimes.com/2017/09/10/your-money/identity-theft/equifax-breach-credit-freeze.html?mcubz=3 [Accessed 18 Sep. 2017].

[13] O'Shea, B. (2017). *Lock Down Your Data After Equifax Breach — Right Now*. [online] NerdWallet. Available at: https://www.nerdwallet.com/blog/finance/protect-yourself-equifax-data-breach/?utm_campaign=cd_mktg_paid_090817_traffic_ccd_equifax_so&utm_source=fb&utm_medium=sc&utm_content=13 [Accessed 18 Sep. 2017

[14] Cole, L. (2017). *The Equifax breach may have exposed 143 million people's Social Security numbers — but here's why you shouldn't freak out*. [online] Business Insider. Available at: http://www.businessinsider.com/equifax-hack-dont-freak-out-2017-9 [Accessed 18 Sep. 2017].

[15] Scott, J. (2017). *Dragnet Surveillance Nation*. [online] Available at: http://icitech.org/wp-content/uploads/2017/01/Dragnet-Surveillance-Nation.pdf [Accessed 18 Sep. 2017].

[16] S. Durbin, "Insiders are today's biggest security threat," Recode, 2016. [Online]. Available: http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin. Accessed: Jan. 22, 2017.

[17] P. Kanagasingham, "Data Loss Prevention," in *Sans Institute*, 2008. [Online]. Available: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883. Accessed: Jan. 26, 2017.

[18] Simon, "Insider threat prevention using a file server in an SMB (small & medium business)," in *Secudrive*, 2016. [Online]. Available: http://www.secudrives.com/2016/11/22/insider-threat-prevention-using-a-file-server/. Accessed: Jan. 25, 2017.

[19] K. Lonergan, "The critical difference between SIEM and UBA - and why you need both to combat insider threats," in *Security*, Information Age, 2015. [Online]. Available: http://www.information-age.com/critical-difference-between-siem-and-uba-and-why-you-need-both-combat-insider-threats-123460054/. Accessed: Jan. 25, 2017.

[21] R. Rose, "The future of insider threats," in *Forbes*, Forbes, 2016. [Online]. Available: http://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#6f5e96cc6726. Accessed: Jan. 30, 2017.

[20] "What is a SIEM?," in Tripwire, Tripwire, 2016. [Online]. Available: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/. Accessed: Jan. 22, 2017.

[22] C. Sherman, "The Forrester Wave™: Endpoint security suites, Q4 2016," 2016. [Online]. Available: https://www.forrester.com/report/The+Forrester+Wave+Endpoint+Security+Suites+Q4+2016/-/E-RES113145. Accessed: Jan. 30, 2017.

[23] "2016 Data Breach Investigations Report," Verizon, 2016. [Online]. Available: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/. Accessed: Jan. 22, 2016.

[24] http://icitech.org/icit-analysis-identity-and-access-management-solutions-automating-cybersecurity-while-embedding-pervasive-and-ubiquitous-cyber-hygiene-by-design/

[25] T. Kemp, "Identity is the new perimeter," 2015. [Online]. Available: http://blog.centrify.com/identity-is-the-new-perimeter-2/. Accessed: Jan. 21, 2016.