# **Equifax Data Breach**

In the years leading up to the breach, Equifax struggled with outdated cybersecurity policies and instruments. In April of 2015, former CSO Susan Mauldin implemented Equifax’s first patch management policy. An internal audit of the policy later that year revealed numerous security deficiencies, including over 8500 unresolved software vulnerabilities (PSI). In May of 2016, Equifax’s W-2 Express website was also hacked, resulting in the leak of 430,000 names, addresses, social security numbers, and other types of personal information (Brewster). By 2017, most of Equifax’s security deficiencies had not been remediated, allowing hackers to breach Equifax’s network and harvest the PII of 147 million consumers’ personal information (PSI).

Events began on March 7th of 2017, when Apache publicized and provided a patch for Apache Struts, an easily exploitable software vulnerability. On March 8th, The Department of Homeland Security’s US-CERT team (a division within the DHS responsible for disseminating information on cyber security threats) notified Equifax of the software flaw, and an alert was distributed to 400 employees by Equifax’s Global Threats and Vulnerability Management (GTVM) team (PSI). Apache Struts was also assigned the highest possible criticality score, a 10, by the National Institute of Standards and Technology (NIST) using the Common Vulnerability Scoring System or CVSS (PSI).

On March 10th, hackers breached Equifax’s networks by exploiting Apache Struts via Equifax’s online dispute portal. On May 13th, attackers spread from the infected portal and gained access to other parts of Equifax’s network (Fruhlinger). From May through July, hackers accessed multiple Equifax databases and extracted consumers’ personal information. Stolen data included consumers’ names, addresses, dates of birth, social security number, and credit card numbers (PSI).

After learning of the breach, Equifax GVTM teams attempted and failed to locate Apache struts on servers by conducting multiple network scans. IT and Security’s inability to locate and patch Apache Struts can be attributed to the existing flaws in their cyber security policy, outlined in a report published by the Senate Subcommittee on Investigations (PSI):

**Lack of Comprehensive IT Asset Inventory**

At the time of the breach, Equifax lacked a complete IT Asset Inventory, meaning they did not know the locations of the Apache struts application on their network. Instead, IT had to conduct network scans, which failed to detect the software.

**Failure to follow Patch Management Policy**

Equifax’s security policy mandated critical vulnerabilities be patched within 48 hours of discovery, but according to Mandiant, the lack of IT Asset Inventory made meeting this deadline impossible. Struts was ultimately patched 5 months after Equifax learned of the flaw. IT conducted multiple network scans but could not find instances of the vulnerable software. After failing to locate the application, IT and security took no further action to find Struts, and management did not check the vulnerability had been remediated.

**IT and Security Management**

Communication among employees on the remediation of security vulnerabilities was inconsistent. Equifax held monthly GMTV meetings to discuss new vulnerabilities, but the status of the previous months’ threats was often not discussed, even if they had not yet been remediated (PSI). Equifax did not require attendance from employees or management or keep records of who attended meetings. Additionally, the only employee who knew of Equifax’s use of Apache Struts in the online dispute portal was not included on the GTVM distribution list and did not receive news of the vulnerability. The senior manager who oversaw this lead developer and his team received the alert but failed to relay the information.

**Failure to Maintain Cybersecurity Technologies**

The severity and duration of the breach was exacerbated by Equifax’s failure to renew an SSL certificate needed to inspect encrypted network traffic. Hackers encrypted their activities on Equifax servers, but because the certificate had expired, incoming traffic was not decrypted, and Equifax had no knowledge of suspicious activities on the online dispute portal.

On July 29th, Equifax renewed the expired SSL certificate designed to inspect encrypted network traffic. IT immediately noticed suspicious activities on Equifax servers, leading to the discovery of the breach (Fruhlinger). On August 2nd Equifax retained law firm King and Spalding LLP, which enlisted Mandiant to investigate the breadth of the breach. Over the next several weeks, Equifax employees identified a list of affected consumers (PSI).

On September 7th of 2017, six weeks after its discovery, Equifax issued a public announcement their networks had suffered a data breach that exposed the personal information of 143 million consumers (Equifax later discovered an additional 4 million affected consumers). Initially many expected the breach would result in widespread identity theft and fraud. Ultimately, investigators came to believe the breach was executed by Chinese state-sponsored hackers as part of a government operation to collect American data (Fruhlinger).

**Outcomes**

**Investigations and Findings**

The Equifax breach was investigated by several Federal authorities, including the FBI, the FTC, and the CFPB. An additional insider trading investigation was conducted by the Securities and Exchange Commission (SEC) and the US Attorney’s office in Atlanta related to the sale of $2 million of Equifax stock by executives after the discovery of the breach. Equifax also faced inquiries by at least 34 State attorney generals (EPIC).

Additionally, members of Congress from the House Financial Services Committee, the Senate Banking, Housing, and Urban Affairs Committee, the Senate Commerce, Science, and Transportation Subcommittee, the House Energy and Commerce Committee, the Senate Banking Committee, and the Senate Judiciary Subcommittee on Privacy held congressional hearings covering the breach (EPIC). The breach was also investigated by the Senate’s Homeland Security Permanent Subcommittee on Investigations (PSI), a subcommittee responsible for investigating government operations, compliance with regulations and laws, and cases of crime and fraud which threaten national welfare (HSGAC).

PSI published a detailed report that concluded the breach was likely preventable and outlined Equifax’s history of lax cybersecurity practices. The consensus of investigations was Equifax was responsible for the loss of PII through negligence.

**Lawsuits**

Equifax faced lawsuits by both local and state governments. The city of San Francisco sued Equifax over violations of California’s unlawful, unfair, or fraudulent business practices law and the city of Chicago sued Equifax over violation of the Illinois Personal Information Privacy Act, the Illinois Consumer Fraud and Deceptive Business Practices Act, and the Chicago Consumer Fraud ordinance (EPIC). Attorney Generals Maura Healey and Curtis Hill also sued Equifax on behalf of their states of Massachusetts and Indiana (Kovacs).

**Resignations**

CEO Richard Smith, CSO Susan Mauldin, and CIO David Webb resigned in the aftermath of the breach (Horowitz & Wiener-Bronner). Smith retained his full pension, valued over $18 million after his resignation (LaMagna).

**Arrests**

In 2019, former Chief information Officer Jun Ying was found guilty of insider trading and sentenced to four months in jail. Former Equifax manager Sudhakar Reddy Bonthu was also found guilty of insider trading and sentenced to 8 months of home confinement. No other Equifax employees faced arrest related to the breach (Musil).

**Equifax FTC Settlement**

In July of 2019, in a settlement with the FTC, the Consumer Financial Protection Bureau, 48 states, the District of Columbia, and Puerto Rico, Equifax agreed to pay up to $700 million in fines and compensation for the 147 million affected individuals. $300 million of the settlement was distributed to individuals whose personal information had been exposed during the breach. Equifax was also required to pay up to $125 million in consumer compensation for additional out-of-pocket losses if needed. Equifax paid $175 million to states and $100 million to the CFPB in civil penalties (FTC).

The FTC alleged that Equifax violated “the FTC Act’s prohibition against unfair and deceptive practices and the Gramm-Leach-Bliley Act’s Safeguards Rule, which requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect the security, confidentiality, and integrity of customer information” (FTC).To address deficiencies in Equifax’s cybersecurity, the FTC also required Equifax instate a comprehensive information security program which would include “annual assessments of internal and external security risks and assure that service providers with access to personal information stored by Equifax also implement appropriate security programs” (FTC).

Several forms of compensation were offered as part of the $300 million paid out to affected consumers (JND):

**Free Credit Monitoring Services**

Consumers who filed a claim within the first claims period (prior to the January 22nd, 2020 deadline) were eligible for 4 years of credit monitoring services provided by Equifax, Experian, and Transunion with up to $1,000,000 in identity theft insurance. After this 4-year period, consumers who successfully filed a claim could enroll in 6 more years of credit monitoring services provided by Equifax.

**Cash Payout**

Within the first claims period, consumers who had already purchased credit or identity monitoring services for at least six months prior to the breach were eligible to claim a maximum of $125 in compensation in lieu of free credit monitoring services.

**Identity Theft Compensation**

Consumers were eligible to receive compensation (up to 20 total hours at $25 an hour) for time spent recovering from identity theft and fraud occurring within the first claims period. Consumers could also claim up to $20,000 in out-of-pocket losses occurring within this period.

**Extended Claims Period Identity Theft Compensation**

While the first claims period has passed, consumers are now eligible to receive compensation for out-of-pocket losses and time spent recovering from identity theft and fraud occurring within the extended claims period of January 23, 2020 and January 22, 2024.

**Identity Restoration Services**

All affected consumers are eligible for Experian’s Assisted Identity Restoration Services if they experience identity theft within seven years of the breach. These services include, “access to a U.S. based call center providing services relating to identity restoration, assignment of a certified Identity Theft Restoration Specialist to assist you in addressing an identity theft event, and assistance with a step-by-step process to deal with companies, government agencies, and credit bureaus” (Equifax).

**Equifax Subscription Product Reimbursement**

Consumers who had an Equifax credit monitoring or identity theft protection subscription between 9/7/2016 and 9/7/2017 were eligible for reimbursement of 25% of the amount paid if they filed a claim within the first claims period.

The terms of the payout garnered criticism by both consumers and lawmakers. Equifax’s settlement with the FTC promised only $31 million in compensation for consumers who had credit monitoring services at the time of the breach, with a maximum payout of $125 per customer. As Senator Elizabeth Warren pointed out, this would only cover the $125 compensation of 248,000 individuals. Because Equifax had millions of qualified customers, the realistic payout would be far lower (Higgins). This turned out to be the case. By the December 2020 deadline, over 4.5 million consumers filed a claim, resulting in an estimated payout of only $7 each (Siegel Bernard). Consumers and lawmakers also accused the FTC of misleading consumers about the size of the cash payout because some materials seemed to suggest that every affected consumer would receive $125 (Higgins). In response, the FTC recommended that consumers elect the free credit monitoring services option instead of the cash payout (FTC).

Equifax was also accused of complicating the claiming process to reduce the number of individuals able to successfully file claims. Affected consumers received an email from the Equifax settlement team that required them to verify they had credit monitoring services in place by October 15th, 2019. Without verification, consumers’ claims would be denied. According to some consumers, the email looked illegitimate, leading many to question its authenticity. The FTC clarified the email was legitimate on their site (Warzel).

**Independent Settlements with States**

Massachusetts and Indiana secured $18.2 million and $19.5 million in settlements with Equifax respectively (Kovacs).

**Legislation**

The FTC settlement resulted in calls for legislation that would increase penalties for CRAs which lost consumer information. In 2018, Senators Elizabeth Warren and Mark Warner introduced the Data Breach Prevention and Compensation Act, which specifically responded to the Equifax breach. The Act would, “give the Federal Trade Commission more direct supervisory authority over data security at CRAs, impose mandatory penalties on CRAs to incentivize adequate protection of consumer data, and provide robust compensation to consumers for stolen data” (Warren). This would include the establishment of an Office of Cybersecurity at the FTC responsible for conducting inspections of CRA’s cybersecurity. The Act would also impose, “mandatory, strict liability penalties for breaches of consumer data beginning with a base penalty of $100 for each consumer who had one piece of personal identifying information (PII) compromised and another $50 for each additional PII compromised per consumer” (Warren).  Under this Act, Equifax would have paid at least $1.5 billion to consumers.

In March of 2018, the Senate passed the Economic Growth, Regulatory Relief, and Consumer Protection Act, which allows consumers free credit freezes and the ability to place one year fraud alerts on their accounts (FTC). However, lawmakers have not made progress in passing a comprehensive reform bill responding to the Equifax breach. The Data Breach Prevention and Compensation Act was reintroduced in 2019, but since then has not further advanced in becoming law.

**Ethics Analysis**

Several unique aspects of Credit Reporting Agencies’ function impact their position in the economic life of American society and on their ethical responsibilities.

1. CRAs have become gatekeepers for essential functions, like finding work, housing, and managing one’s money. Consumers need credit to navigate the current economic system. While we might be able to choose not to shop at Amazon, for example, electing not to establish a credit history amounts to opting out of regular economic activity. Consumers therefore lack agency in their relationship with CRAs.
2. Information held by CRAs, including PII, is especially sensitive. Other businesses wouldn’t have access to this type of data. Loss of PII can result in identity theft with devastating effects, including financial instability, and lack of access to housing and employment, for consumers. Further, this loss of PII means credit information supplied to lenders is no longer reliable or valuable.
3. Loss of information through data breaches not only threatens the validity of the credit reporting industry’s function but also threatens the United States’ national security and economic infrastructure. The current banking and taxation system utilizes social security numbers as PII. According to security investigators, the Equifax data breach was most likely the work of the Chinese government as part of a scheme to collect pools of consumers’ data. It’s not a stretch to imagine that a hostile international actor could use consumer data to significantly disrupt these systems.

In sum, the position CRAs hold in the US economy, the sensitivity of the information they have access to, and the serious consequences of loss of this data, heighten Equifax’s responsibility to the American public. These factors must be considered in examining the ethics of their behavior.

**1. Promises and Trust: Failure to Protect Consumer Data**

A company has an ethical duty to honor promises made to customers. This kind of promissory obligation is based on commitments to providing certain services and following a code of ethics and conduct. According to business ethicists like Manuel Velasquez, these promises can be understood as a kind of contractual relationship between a customer and a corporation (Velasquez). We require higher standards of performance from individuals and companies making these promises because clients put their trust in those individuals or companies based on these “contracts.”

Equifax’s failure to protect consumer data falls broadly into the category of negligence. Equifax IT and Security failed to adhere to cybersecurity policies specifically designed to prevent data breaches. Several contextual factors contribute to the ethical assessment of negligence:

1. The potential consequences of negligence

For example, negligence in a trivial matter such as sorting recycling, would be weighed as far less morally repugnant than forms of negligence that could end another person’s life. Equifax’s failure to follow cybersecurity policies jeopardized the PII of millions of Americans with potentially catastrophic personal consequences as well as posing a continued threat to national security.

1. Whether negligence was part of a pattern of behavior

During a senate testimony Former Equifax CEO Richard Smith blamed the breach on the actions of one security employee, who he reported was meant to apply the patch, but didn’t (Siegel Bernard & Cowley). However, the root of Equifax’s cybersecurity problem actually lies in management’s failure to create a robust patch management policy and culture of proactive and thorough cybersecurity. In a company managing thousands of employees, a reliable corporate policy should have back-up protocols to prevent the human error of one individual causing the collapse of the system. In 2015, years before the breach, Equifax’s management was made aware of systemic flaws in their patch management policy which left thousands of critical vulnerabilities unpatched (PSI). The Equifax breach was therefore the consequence of a formally acknowledged pattern of behavior.

1. Whether negligence was ‘knowingly’ committed

An individual who acts carelessly, knowing she is taking a risk and understanding the possible consequences is judged more seriously than someone who acts carelessly due to forgetfulness or ignorance. Equifax management and employees were notified of the Apache Struts vulnerability by US-CERT, and NIST assigned the vulnerability the highest severity score possible, a 10. Equifax’s GTVM team circulated the notification to over 400 company employees following the alert (PSI). Equifax management knew of the risk Apache Struts posed as well as the ongoing risks associated with lax cybersecurity practices.

1. Whether a company has made a promise to take certain precautions as part of a professional code

A higher standard of caution is generally required from professions or businesses that promise to abide by a code to protect their clients from harm.  A physician who is careless with his patients’ health, by not checking their history of allergies before administering medications is subject to moral censure as well as the loss of license to practice. The fact this physician has sworn an oath to protect patients’ health makes carelessness even more damning. Equifax promises consumers it will protect PII and provide accurate and fair credit reports (Equifax). Thus, Equifax breached consumers trust in two ways. Firstly, Equifax clearly broke its promise to protect consumer data by failing to follow cybersecurity policy. Secondly, Equifax’s negligence created the conditions for widespread identity theft which could undermine the validity of credit information and jeopardize its promise to provide accurate and fair credit reports.

Thus, the severity of Equifax’s negligence makes this breach of trust especially difficult to accept and demonstrates Equifax’s culpability in the loss of consumer information.

**2.Transparency:Failure to Report the Data Breach in a Timely Manner**

Consider the maxim or statement, “Companies will lie to consumers to make more money.” Using Kantian moral reasoning, we can universalize this statement by imagining a world in which people always deceive each other for personal benefit. If we apply this maxim in this imagined world it creates a contradiction: In a world where people couldn’t make promises, how would a company deceive consumers? If companies lied consistently, trust between consumers and companies would be completely degraded. This maxim becomes irrational when made into a universal law of nature and is therefore unethical (Johnson & Cureton).

Thus, companies like Equifax have a duty of transparency. Even if customers are not directly lied to, withholding information that impacts the company’s ability to deliver on promises and may cause customers serious harm is also dishonest and unethical. Applied to CRAs, this creates a duty of timely disclosure of data breaches.

Equifax waited six weeks after its discovery of the breach to alert customers that their PII had been compromised. In most data breach cases, companies might take time to investigate the cause, identify affected consumers, and prepare a plan of remediation, but Equifax executives never explained the reasoning for their timeline (Tsukayama). During this six week period, it can be assumed management strategized on minimizing fallout and public scrutiny, choosing to prioritize the company’s reputation over the continued risk to millions of customers.

Equifax executives also sold $2 million in Equifax stock shortly after the breach was discovered. Individuals with influence in Equifax’s administration used their private knowledge of the breach for personal gain, while affected consumers had no opportunity to protect themselves from the potentially devastating effects of the loss of their personal information. Thus, executives valued the bottom line and their personal financial status over their duty to transparency.

**3. Justice and Fairness: Lack of Compensatory Justice**

Finally, companies have an ethical duty to follow principles of justice in compensating consumers for inflicted harm. Aristotle’s theory of corrective justice, concerned with the relationship between wrongdoer and victim, demands that “fault be cancelled by restoring the victim to the position she would have been in had the wrongful behavior not occurred” (Miller).  The ultimate goal of corrective justice is to adequately reduce or reverse inflicted harm.

Equifax inflicted harm on consumers by failing to protect their PII and jeopardizing their financial security. Even if consumers didn’t experience identity theft immediately after the breach or within the extended claims period, in a digital age, loss of personal information is permanent. Consumers’ PII could still be exploited in future with little recourse.

The value of the FTC mandated cash payout did not match the severity of these injuries. The value of protecting personal information is far greater than $7 or even $125 dollars. This is demonstrated by Equifax’s own credit monitoring rates, which cost around $20 a month (Equifax). If greater numbers of consumers filed cash payout claims, the payout value would have been reduced to mere cents. Equifax’s settlement fund was not large enough to ethically compensate consumers for harm done, and thus corrective justice was not achieved. It is nearly impossible to value the price of personal information, but clearly, Equifax valued the company’s financial welfare over consumer compensation. Equifax suffered significant reputational damage as a result of the breach but has since recovered materially with few long-term consequences to their business. In 2018 and 2019, Equifax reported revenues of $3.41 and $3.5 billion respectively (Equifax).

While the free credit monitoring services offered were clearly a better deal than the cash payout, once the 10-year service period is complete, consumers will once again have to purchase credit monitoring services to regularly view their credit. The extended claims period in which consumers may be compensated for identity theft and fraud associated with the breach only lasts for an additional four years. Even though consumers’ PII are permanently lost, settlement terms do not compensate consumers in a long-term manner.

Finally, distribution of consumer compensation was poorly managed. The goal of compensatory justice is to reduce harm done to as many individuals as possible, but the FTC’s unclear representation of settlement terms and Equifax’s confusing communications with consumers made it more difficult for them to claim deserved compensation.

**Policy Recommendations**

The Equifax data breach should spur US regulatory agencies and the legal system to take seriously the responsibility to protect consumers from negligence and other wrongdoing by companies. The ethical failures in this case suggest the US regulatory system is inadequate as it pertains to the credit reporting industry. To prevent future breaches of this kind and properly compensate consumers for loss of PII, Congress should pass legislation that will:

1. Increase regulation of CRAs cybersecurity practices

CRAs privacy practices should be regulated by an external body in the same way as other financial institutions. As senators Warren and Warner suggested, creating a division of the FTC specifically responsible for monitoring CRAs cybersecurity practices might prevent the kind of negligence in the Equifax breach by ensuring consumer data are adequately protected at all times.

1. Improve breach notification laws

CRAs should be legally required to notify the public of data breaches within a few days of their discovery to reduce harm to consumers resulting from loss of PII.

1. Increase consumer compensation for loss of PII

CRAs should provide consumers with increased monetary compensation based on the quantity of PII lost. As senators Warren and Warner have argued, if consumers’ personal information is properly valued, CRAs will be incentivized to protect consumer data to avoid financial losses. Further, if a breach does occur, consumers will be justly compensated for harm done.