

The 2017 Equifax Data Breach

Samuel Woodruff

Department of Cybersecurity, Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

February 1, 2026

In 2017, Equifax, one of the three major credit reporting bureaus in the United States, experienced one of the worst data breaches in recent memory. Being one of the largest credit bureaus in the United States, the data breach exposed the sensitive financial and personal information of millions of Americans. The breach exposed key flaws in Equifax's security which largely included unpatched software and poor monitoring. As a result, public trust in Equifax was significantly eroded and the company was brought under major scrutiny.

The Equifax data breach was the result of a few different key vulnerabilities but most notably a vulnerability in an unpatched version of the Apache Struts software. This vulnerability in the Apache Struts software was discovered in March of 2017 and Equifax's Global Threat and Vulnerability Management (GTVM) notified individuals throughout the company of the vulnerability shortly thereafter. However, despite Equifax's GTVM notifying the company to update their systems, Equifax did not fully patch all systems using the vulnerable Apache Struts software. The primary system hackers exploited was Equifax's Automated Consumer Interview System which was left unprotected and running the vulnerable, older version of the Apache Struts software. According to the House Committee on Oversight and Government Reform, hackers "...found a file containing unencrypted credentials..." and then "...were able to use these credentials to access 48 unrelated databases" within Equifax's network. (House Committee on Oversight and Government Reform, 2018). This highlights an additional vulnerability with Equifax's network being a lack of segmentation throughout as hackers were able to access numerous unrelated databases. One last vulnerability of Equifax's systems exposed by the attack was their monitoring services. According to Josh Amishav of Breachsense, the network monitoring services that Equifax used weren't working at the time of the breach due to "A critical SSL certificate had expired in January 2017" and thus, "the monitoring tools

couldn't decrypt traffic" (Amishav 2026). All of these different vulnerabilities helped to come together and contribute to one of the worst data breaches of all time.

In the wake of the Equifax data breach, millions of people were left wondering who committed the attack and how. The main method hackers used to gain access to millions of individual's information was through the unpatched version of Apache Struts found within Equifax's Automated Consumer Interview System. From there, hackers were able to use stolen credentials to access several different unrelated databases to steal information. Due to the SSL certificate being expired, hackers were able to go undetected in Equifax's systems until the certificate was renewed in July, 2017. Once the certificate was renewed, "Equifax observed additional instances of suspicious traffic originating from a second IP address owned by a German ISP, but leased to a Chinese provider" (House Committee on Oversight and Government Reform, 2018). This discovery led to Equifax taking down the Automated Consumer Interview System which only then revealed the true damage of the attack. The U.S. Department of Justice later charged Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei with responsibility for the Equifax data breach. The U.S. Department of Justice alleged that these four "...were members of the PLA's 54th Research Institute, a component of the Chinese military" (U.S. Department of Justice, 2020). The data from the Equifax data breach notably never appeared for sale on the dark web, which Josh Amishav says points towards "...nation-state operations focused on intelligence gathering rather than quick financial gain" (Amishav 2026).

What makes the Equifax data breach so notable are its repercussions. Around 147 million Americans had sensitive information including social security numbers, driver's license numbers, credit card information, and more. Due to Equifax's negligence in the situation, the company had to reach a settlement with multiple legislators and agencies. According to

Breachesense, the settlement included “...\$700 million to settle with the FTC, CFPB, and 50 state attorneys general” and “...included \$425 million for consumer compensation” (Ashimav 2026). Additionally, several executives of Equifax either resigned or retired shortly after the incident.

There were several measures that could have been taken to mitigate or prevent the Equifax data breach altogether. One rather simple measure the company could have taken is to set reminders for when certificates are going to expire so that they may be renewed in time. Doing this alone would have helped the company detect the anomalous activity. Equifax also could have segmented their network further so that hackers would not be able to use the same credentials to access unrelated databases. Lastly, additional forms of multifactor authentication could have been used so that compromised credentials could be differentiated from authenticated use.

Overall, the Equifax data breach was one of the most consequential breaches of modern history. It affected an unprecedented amount of Americans, leaving their identities exposed and vulnerable. Equifax operated negligently which helped contribute to many of the vulnerabilities that were exploited in the attack. As a result, millions of Americans were left vulnerable and Equifax was left to pay hundreds of millions in settlement fees. By adhering to cybersecurity policy and implementing different mitigation techniques, the Equifax data breach could have been prevented altogether. All of these reasons are why the Equifax data breach remains one of the most infamous cases of data breaches in modern times.

Works Cited

Amishav, J. (2026, January 26). *Equifax data breach 2017: Timeline, costs & security lessons*.

BreachSense. <https://www.breachsense.com/blog/equifax-data-breach/>

U.S. Department of Justice. (2020, February 10). *Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax* [Press release].

<https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking>

House Committee on Oversight and Government Reform. (2018). *The Equifax data breach: Majority staff report* [PDF]. U.S. House of Representatives.

<https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>