The Equifax Security Breach of 2017: Vulnerabilities and Impact

Sean M. Shreve

Old Dominion University

CYSE-300: Introduction to Cybersecurity

Dr. Joseph Kovacic

07 September 2025

The Equifax Security Breach of 2017: Vulnerabilities and Impact

In 2017, the American credit reporting agency Equifax was hacked by members of China's 54th Research Institute, a branch of the People's Liberation Army (U.S. Department of Justice, 2020). Vulnerabilities of Equifax's cybersecurity were exposed and the personal data of nearly half the United States' population was compromised. This event remains to date the largest cybersecurity attack Equifax has faced, and also one of the largest in United States history. The country shifted into reform in many legislative circles of government in regards to cybersecurity and consumer private information protection. Equifax also faced several penalties and repercussions from their failures in cybersecurity practices. Ultimately, the Equifax breach stands as a case study of how neglected information system security can devastate both consumer trust and corporate integrity.

Rather than a direct break in their security system, Equifax produced their own vulnerability that lead to the breach. On March 8, 2017, the Department of Homeland Security (DHS) gave official notice to Equifax that Apache Software reported a vulnerability and had a patch available (Mozilla, n.d.). Apache, specifically Apache Struts, is a web application framework used to build and maintain websites. This notice was provided only one day after Apache Software discovered the vulnerability, however, Equifax never patched their framework. The hack occurred on May 13, 2017 by four members of the Chinese People's Liberation Army (PLA), over two months pass the initial noticed submitted by the DHS (U.S. Department of Justice, 2020). Motivations for such a hack are many, however the data that was compromised has yet to appear on the black market, and now is being assumed to be used for espionage (Mozilla, n.d.). The Chinese government has denied the accusations to this day, however the

official press statement from the Department of Justice in 2020 specially names four members responsible for the hack (U.S. Department of Justice, 2020).

What were the repercussions of the breach?

The repercussions of this breach have been massive across multiple areas. By exposing personal identifying information, the incident placed an estimated 145 million people at risk of identity theft and fraud (U.S. Department of Justice, 2020). This prompted U.S. government response, at both the state and federal levels. Equifax officially announced the hack on September 7, 2017 through Twitter, just under four months since the breach (Mozilla, n.d.). Within a year, nine U.S. states either introduced new bills or amended older laws to strengthen enforcement of notifications of future breaches (Wear et al., 2018). Equifax also entered into a settlement in July of 2019, involving all 50 U.S. states and territories, also including the Federal Trade Commission and the Consumer Financial Protection Bureau (Federal Trade Commission, 2019). The company settled in 2019, which led to payments of up to 700 million dollars, along with services such as identity recovery assistance and free credit monitoring (Mozilla, n.d.).

The most critical cyber security measure that should have been used to prevent the incident would be the immediate patching of the vulnerability. The time between being notified by the DHS and applying the patch was four months. This is widely considered an unacceptable amount of time for this action due to the kind of information being exposed. The consumers should have also been notified much sooner about their information being leaked. This would have provided them time to take protective measures against possible identity theft or at the least establish safeguards. Appropriately, this was also part of the settlement mentioned before; which provides free identity restoration services for up to seven years (Mozilla, n.d.).

The Equifax breach is a landmark case in the critical importance of cybersecurity and how lax practices in its upkeep can cause devastating damage. It spurred reform in many sectors of policy, from stronger consumer notification policies to enhanced protections of personal identifying information (Wear et al., 2018). Repercussions for Equifax were significant. Leadership changes, fines for nearly one billion dollars, and more of company's resources have been designated for consumer information recovery and support (Mozilla, n.d.). Ultimately this incident stands as a defining moment in U.S. cybersecurity history, showing as an example how neglected information system security can be immensely detrimental to public trust and business integrity.

References

Federal Trade Commission. (2019, July 31). *Federal Trade Commission v. Equifax, Inc.* (Matter/File No. 172-3203). In *FTC legal library: Cases and proceedings*. https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc

Mozilla. (n.d.). *Equifax data breach: A look at how it happened*. Mozilla Monitor. Retrieved September 6, 2025, from https://www.mozilla.org/en-US/products/monitor/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 Equifax* [Press release]. U.S. Attorney's Office, Northern District of Georgia. https://www.justice.gov/usao-ndga/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud

Wear, J. D., Flowers, R., Black, K. D., Godfrey, L. D., & Anderson, R. D. (2018). RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY. *Tort Trial & Insurance Practice Law Journal*, *53*(2), 291–314. https://www.jstor.org/stable/27172756