# Equifax 2017 Breach

Adeline Harris

School of Cybersecurity, Old Dominion University

CYSE300: Introduction to Cybersecurity

Professor Kovacic

January 26, 2025

It is of utmost importance that cybersecurity is ensured in today's world, where data and information are greatly increasing and readily available through the internet. Sensitive and confidential data belonging to companies and individuals are constantly targeted by malicious actors for theft, damage or alteration. This paper explores one of the most significant data breaches in recent history, The 2017 Equifax Breach, which compromised personal and financial data affecting millions of individuals in the United States. The breach resulted in the exposure of personal identifiable information (PII) of approximately 147 million people. This paper examines the agency, the cause of the breach, its repercussions, and lessons learned to prevent future incidents.

Equifax is one of the major credit reporting agencies founded in 1899, and headquartered in Atlanta that provides records of individuals' credit standing, if they are up-to-date on their loan and credit card payment. They gather their information from financial companies, employers and consumers. Equifax records are looked up to verify whether an individual has a history of repaying when they apply for credit (Epic, 2021). As of 2016 reports, the agency organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide (Kabanov & Madnick, 2021). In its business as a credit reporting agency, Equifax houses the personal information of nearly every adult in the U.S. banks, employers, and lenders use its data to verify identities, approve loans, and for other everyday purposes (Epic, 2021). Because of their operation, the agency possesses a vast amount of sensitive data making it a target for cybercriminals looking to steal identities, due to the agency dealing in the personal identifiable information of such a large number of people. The agency treated its consumers as clients, meaning all data buyers also had their information in the databases. At the time of the breach the CEO of Equifax was Richard Smith who took on the role in 2005. The chief security officer was Susan Mauldin and she was also the first CSO to implement the patch management policy. Their chief information

officer was David Webb, who got appointed in the position in 2010. The company dealt with a variety of customers, ranging from other companies and businesses that requested credit reports of their consumers or other businesses, to members of the public who requested credit reports or sought information on their own credit rating. Equifax worked with the Federal Trade Commission to uphold the Fair Credit Reporting Act (FCRA). This act ensures accurate, fair and private handling of consumer credit reports. It also stated that, in line with fairness, consumers had access to a free credit report every twelve (12) months. In working with the rules of the FTC, they also had to work with another government agency called the consumer financial protection bureau (CFPB), which assisted the FTC to regulate CRAs through provisions set by the Dodd-Frank Wall Street Reform and Consumer Protection Act. This act was designed to prevent unfair and deceptive acts by the agencies, and to ensure they provide meaningful and accurate credit ratings of all the clients they evaluate. The CFPB may also have the authority to examine and supervise the CRAs activities. These associations coupled with a few other facts put Equifax amongst the top brass of their industry, as they along with Experian and Transunion were referred to as the big three (Miyashiro, 2021). This made it a trusted CRA which is why it had a very large customer base and why its breach is considered as one of the largest information breaches in the world.

Equifax, like other CRAs, had a history of poor cybersecurity practices, contributing to the breach. A critical vulnerability was failing to renew their secure socket layer (SSL) certificate on their SSL visibility appliance, a tool that inspects encrypted inbound and outbound network traffic. According to reports from November 2016, the certificate had expired 9 months prior to their discovery that the attack had already occurred (Kabanov & Madnick, 2021). This time lapse prevented the system from inspecting incoming network traffic, allowing malicious activity to go undetected. It was only after renewing and updating the certificate that their IT staff detected unusual activity on the servers when the network started

decrypting incoming traffic (Epic, 2021). The attack was considered an Advanced Persistent Threat (APT) attack, where the attacker gained access and remained undetected for a period of time. The attackers gained access to their Automated Consumer Interview System (ACIS) and databases containing consumers' personal data, exfiltrating that data over a period of 78 days before detection (Kabanov & Madnick, 2021). The actors behind this attack were state-sponsored hackers allegedly tied to China. These attackers exploited a vulnerability in the Apache Struts CVE-2017-5638 web application framework, allowing them to issue commands to the server remotely (Epic, 2021). Since the company did not regularly perform patch management the breach was not identified or stopped even after Apache fixed their vulnerability that allowed malicious code to be inserted in the content-type header of the HTTP requests (Epic, 2021). The attackers exploited the vulnerability and gained access to the system due to hierarchical system failures that resulted from the outdated software (Kabanov & Madnick, 2021). The incident has served as a major learning instrument for individuals and businesses alike.

This breach resulted in the theft of highly sensitive data including Social Security Number, Name, Date of Birth, Addresses Driver’s License Number, and credit card information. It affected nearly half of the United States, approximately 147 million individual’s privacy was violated putting them at risk for financial fraud and identity theft. Equifax faced serious financial losses due to fines, lawsuits and settlements. Both the local and State government filed lawsuits against the agency. According to San Francisco, Equifax violated California’s unlawful, unfair or fraudulent business practices law by failing to implement and maintain security practices, failed to provide timely notice of the breach and failed to provide clear and complete information. Chicago claimed it violated Illinois Personal Information Privacy Act, the Illinois Consumer Fraud and Deceptive Business Practices Act and the Chicago Consumer Fraud ordinance (Epic, 2021). The incident brought damage to the agency's

reputation when the story broke on news media such as CNN and New York Times which caused the executives to face inquiries from FBI, FTC and the Consumer Financial Protection Bureau (CFPB) (Team, 2024). Adding to their damaged reputation, the agency had to deal with the resignation of the CEO and a few executives, while the CEO retained his full pension valued at over $18 million. Additionally, Equifax's $125 million cybersecurity insurance policy was insufficient to cover the breach, forcing the company to spend an additional $1.4 billion on cleanup and IT system improvements. A class-action lawsuit with the Federal Trade Commission (FTC) resulted in a $1.38 billion settlement to address customer claims (Miyashiro, 2021).

As is the case with any breach, many lessons were learned. The need for security patches to be downloaded and installed immediately as it is released became apparent. It is also recommended that a multifactor authentication or zero access authorization tool be used to detect unauthorised access (Epic, 2021). These approaches will help keep data safe, but other actions, such as Granular access control that permits access based on role, real-time access request that grant on deny access in real time, and comprehensive audit logs that shows when, for what, and by who data is accessed, can also help ensure the system is not breached (Epic, 2021). Another approach that can be taken especially at the start of setting up a network for individual or business use is to hire professional security experts, perform penetration tests and zero day tests. These are a few recommended approaches, among others, that can be taken to prevent breaches like this.

The Equifax breach was one of the biggest data breaches in the world. It occurred in May of 2017 and was not detected till July due to a lack of patch management policy in the company. It affected a lot of individuals and cost the company a lot but has become a prime learning experience that helps other companies build better security systems.

**Reference**

Miyashiro, I. K. (2021, April 30). *Case study: Equifax Data Breach*. Seven Pillars Institute. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

Epic. (2021). *EPIC - Equifax Data Breach*. Archive.epic.org; Electronic Privacy Information Center. https://archive.epic.org/privacy/data-breach/equifax/

Team, S. (2024, December 20). *Equifax Data Breach: What Happened and How to Prevent It*. Strongdm.com; StrongDM, Inc. https://www.strongdm.com/what-is/equifax-data-breach

Kabanov, I., & Madnick, S. (2021). Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense. *MIS Quarterly Executive*, *20*(2), 109–125. https://doi.org/10.17705/2msqe.00044