**Equifax (2017) – Breach Summary Case File**

## Background

Equifax is one of the largest consumer credit reporting agencies in the United States. In 2017, the company experienced one of the most devastating data breaches in U.S. history, exposing the personal information of nearly 150 million Americans. This breach not only revealed systemic security failures within Equifax but also heightened public and regulatory attention to the importance of data protection in the financial sector.

## Narrative of the Incident

The breach occurred due to a failure to patch a known vulnerability in Apache Struts, a widely used open-source web application framework. In March 2017, the U.S. Department of Homeland Security notified Equifax of the critical vulnerability (CVE-2017-5638) and urged all users to apply the patch immediately. Despite this warning, Equifax failed to update the affected system in a timely manner.

In May 2017, attackers exploited the unpatched vulnerability to gain access to Equifax's systems. They remained undetected for over two months, exfiltrating sensitive data including:

- Names
- Social Security numbers
- Birth dates
- Addresses
- Driver's license numbers
- Credit card numbers (for approximately 209,000 individuals)

Equifax discovered the breach on July 29, 2017, but did not publicly disclose it until September 7, drawing widespread criticism for the delay. The breach affected nearly half the U.S. population and had far-reaching consequences for consumers and the financial industry.

## Consequences and Impacts

- **Massive data exposure**: Personally identifiable information (PII) of 147 million individuals was compromised.

- **Regulatory and legal consequences**: Equifax faced dozens of lawsuits, government investigations, and was ultimately fined **$700 million** as part of a settlement with the FTC, CFPB, and state attorneys general.
- **Reputational damage**: The breach severely damaged Equifax's public standing and consumer trust.
- **Executive resignations**: The CEO, CIO, and CSO all resigned in the wake of the incident.
- **Policy changes**: The breach prompted stronger data privacy regulations and greater scrutiny of patch management practices.

**Reflection Questions**

As you review this case, consider:

- How did a failure in basic patch management lead to such a large-scale breach?
- What types of data were exposed, and what are the potential consequences of this exposure?
- How did Equifax's response to the breach affect public perception?
- What security controls or organizational processes were missing or failed?
- How does this incident illustrate vulnerabilities in both technical and procedural aspects of cybersecurity?
- Which aspects of the CIA Triad were most affected?

Use this narrative as the basis for your Lab 2 CIA Triad analysis. You are encouraged to cite specific parts of this case file as evidence in your report. You should also go beyond this narrative and seek additional information about this case from reliable external sources, as it is a well-documented cybersecurity attack.