# LESSONS FROM THE EQUIFAX DATA BREACH

Reetuparna Dutta
*Cybersecurity & Privacy Alert*
December 17, 2018

On December 10, 2018, the House Oversight and Government Reform Committee Republicans released a report on the Equifax data breach. The data breach, which Equifax announced in September 2017, ultimately affected 148 million individuals and involved the compromise of personal information including Social Security numbers, addresses, and credit card numbers. The breach resulted from a cyberattack, which started in May 2017 and lasted for 76 days, with hackers trying to obtain remote control over the company's network. The hackers ultimately found a file containing unencrypted credentials, which allowed them to access multiple databases. After obtaining personal information from these databases, the hackers moved the data out of Equifax's system, which Equifax did not realize because the device used to monitor network traffic had been inactive due to an expired security certificate. It wasn't until July 2017 that Equifax updated the certificate and noticed the web traffic.

The Committee found that this breach was entirely preventable because Equifax failed to appreciate and mitigate its cybersecurity risks. It noted that the company did not implement clear lines of authority within their IT department, leading to a gap between policy development and operation. This critical gap led to the company allowing multiple security certificates to expire. The company also failed to implement updated IT systems, which the Committee blamed on an aggressive growth strategy, which involved the company's acquisition of multiple companies with different IT systems. And, after the breach occurred, the company was unprepared to support affected consumers. Its dedicated breach website and call centers were overwhelmed, leaving consumers without the ability to timely obtain information about their vulnerabilities.

While few companies hold the amount of data that Equifax does, the deficiencies in Equifax's IT security were basic and easily fixed. Simply ensuring security certificates were up to date could have prevented this massive breach. Equifax is an example of why companies that hold any personally identifiable information – regardless of volume – must be vigilant in protecting the data and seeking regular assistance in ensuring that they are using the best methods available to protect their customers.

Here is a link to the Committee's Report: https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

### Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Michael Flanagan
Michelle Merola
R. Kent Roberts
Gary Schober
Amy Walters

### Practices & Industries

Business Litigation
Corporate Governance & Compliance
Cybersecurity & Privacy
Intellectual Property & Technology
Technology