The Equifax Data Breach

Mark Wassef

CYSE 300

The Equifax Data Breach of 2017 is considered one of the biggest data breaches in history, approximately 147 million people’s data was leaked in one form or another, ranging from their dates of birth, social security numbers, physical addresses, and other information that might lead to identity theft and fraud. This breach by category is an incredible failure, due to Equifax possessing so much client data, much of the clients affected by the data breach were people who had bought products such as credit scores and credit monitoring which rings as ironic given the circumstance that occurred as a result. Hackers stole 145.5 million Social Security numbers, as well as 209,000 payment card numbers and expiration dates.

The FTC stated that Equifax failed to patch its network despite being alerted in March of 2017, when its team noticed suspicious activity and alerted upper management. An investigation took place and it was revealed that multiple hackers were able to exploit the ACIS vulnerability to cause said data breach, all of the information was revealed to the hackers in plain text. This information helped hackers gain access to a copious amount of consumer data. This occurred within Equifax’s network for months, completely undetected. The ACIS vulnerability was not patched up until July of 2017, effectively giving hackers free reign for 4 months.

The hackers were able to access all this data due to Equifax failing to have protocol for the simplest of security measures. For example, Equifax had no protocol to handle security vulnerabilities in a timely manner, allowing the vulnerability to run for months before being patched. They also failed to segment their database servers to block parts of the network from being hacked, instead, keeping them all unified and more prone to data collection.

Despite these basic measures not being in place, Equifax stated in their privacy policy at the time that they limited their client’s personal information through reasonable procedure, safeguarding their data, this effectively proves that not only was Equifax not properly protecting their consumer data, but they were also lying to their clients about it through their agreements.

As a result, Equifax has settled and agreed to certain conditions including designating an employee to oversee the information security program, conducting annual assessments of internal and external security risks, etc. Equifax also agreed to pay a fine of 575 million dollars. Equifax has pledged to be more stringent with their security, however, public trust has faltered due to this data breach.

References

Staff in the Office of Technology. (2023, June 2). *Equifax to pay $575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

Dohn, K. (2017, September 9). *Identity theft protection following the equifax data breach*. Consumer Financial Protection Bureau. https://www.consumerfinance.gov/about-us/blog/identity-theft-protection-following-equifax-data-breach/