Equifax Data Breach Paper

GBA- 327- CA03

Professor Regan

April 16, 2018

Betsy Posadas, Joshua Holton, Peyton Keith, & Vanna Davis

Equifax Data Breach

Equifax is one of the three credit union companies; the others being Experian and TransUnion. The company's headquarters is in Atlanta, GA, but it has operations all over the world. Equifax helps consumers with their businesses and personal decisions by providing financial support. "On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files (Consumer Notice)." Once the security breach was brought to the public, the company took measures to stop it by conducting investigations and research to see what exactly happened and what data was impacted. This incident was no doubt a crushing blow to internet privacy and the way Equifax handled the situation would become rife with criticism from many sides. In the following paper we will dive a bit deeper into what occurred, how it occurred, who it affected, how the situation was handled initially, and what Equifax is doing today to win back their customers' trust.

The Equifax breach was one of the largest security breaches in America (other clients in other countries were also affected in the UK and Canada [1]) with around 148 million American's [1: Washington Post] private information stolen by cybercriminals. Before the infamous May breach, the company had had a previous prolapse in security in 2016 where Equifax was infiltrated by cybercriminals through the back door of their system. This backdoor was created by Equifax for easier access to their system for their employees and technicians. However, the public could easily access this back door as well [5] [1]. Equifax was warned about these possible outdated security systems which could lead to breaches from hackers and other cybercriminals but ultimately ignored such advice or merely procrastinated on updating their hardware and software [5]. In November 2015, Equifax was sued by several individuals because Equifax violated laws which require institutions to protect consumer information. They

reportedly did not take necessary action to keep up with security that protected vital consumer information [5]. This and other security failures would not be addressed until mid 2017 when a large bulk of American information would again be infringed upon.

The infamous Equifax breaching occurred in May 2017, however notifying the public or government authorities of this information wouldn't be made until July. In addition to that, Equifax wasn't even the first to publicly report the story. In fact, Bloomberg News was the first to notify the public (only banks and important figures knew of the breach at the time.)[Forbes News] As mentioned earlier, the number of consumers affected is about 148 million, including 15.3 million British and 8,000 Canadians information compromised as well [5]. The hackers compromised valuable information such as people's names, birth dates, and addresses. Equifax at first only reported that names and partial driver license numbers were compromised. This would later be revised (with much scrutiny) that the consumers entire driver license information, social Security Card, user's passwords and usernames for their accounts affiliated with their banks, Equifax and other credit companies were compromised and available on the internet.

Now the company must analyze the identify stolen data and other information that was not obtained by the attackers to be able to make connections. The 148 million people that were affected were due to the failure of the company to keep its computer systems up-to-date frequently [3]. Former Chief Executive of Equifax would claim that an individual of the company is to blame for not implementing up to date software patches that would halt any loophole attacks and other techniques used by cybercriminals and hackers [5]. There appears then to be acceleration in the growth of new names to the list of people who got impacted by the hackers.

Equifax`s handling of the situation is regarded as careless as they were not quick to inform consumers on what was stolen. They also lobbied federal regulators and members of Congress to relax Consumer protection laws [6]. House Representative Barry Louder milk would introduce a bill that would limit consumer rights and protections and add a cap to how much a company can be sued for to only 500,000 dollars and eliminate all punitive damages. This bill was pushed before the breach was made public [6].

The company was subsequently faced with backlash and criticism for the way they handled the situation. Lobbying politicians to reduce consumer protection and reducing payments due to damages. Three Equifax executives even sold their holdings of the company after the breach was finally detected [4]. Ultimately, Equifax has only answered partially to Congress and an investigation [1]. They have also used bogus phone numbers and websites to redirect consumers.

Since the attack, according to an update on Equifax's website dated March 1, 2018, the company has stated they have identified at least 2 million American consumers whose information was stolen ("Equifax" 2018). The company claims they are contacting those consumers and offering them "identity theft protection and credit file monitoring services at no cost to them" ("Equifax" 2018). In the statement they go on to say that they are still working diligently to identify and inform the remaining consumers who have been affected. They also say that they are "committed to regaining the trust of [their] consumers, improving transparency, and enhancing security across [their] network" ("Equifax" 2018).

In addition to several other things, Equifax claims, the company has created a web portal that advises their U.S. consumers to recognize any unauthorized activity, review their credit reports and account statements, and "protect their personal information from further attack"

("Equifax" 2018). To this day, the company believes they have met all the suitable requirements in notifying their consumers.

In conclusion, it is without a doubt that the Equifax data breach was one of the biggest cybersecurity scandals to affect U.S. consumers. We know that the breach occurred due to a flaw in the company's system, almost 150 million users were affected, much criticism was given to the company in how they handled the breach, and what the company is doing in 2018 to amend the situation and win back their consumers' ease of mind. Let this be a big lesson to other businesses: if you have, oh let's say, *around 150 million user's worth of personal information*, you should probably take all the necessary steps and actions to ensure those users' safety and privacy.

References:

[1] Consumer Reports. (2018). Equifax Data Breach Affected 2.4 Million More Consumers. Retrieved April 16, 2018, from https://www.consumerreports.org/credit-bureaus/equifax-data-breach-was-bigger-than-previously-reported/

[2] "Consumer Notice - Cybersecurity Incident & Important Consumer Information | Equifax."2017 Cybersecurity Incident & Important Consumer Information, www.equifaxsecurity2017.com/consumer-notice/

[3] Fung, B. (2018). Equifax's massive 2017 data breach keeps getting worse. Retrieved April 16, 2018, from https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.ea5b0f1ed098

[4] Gressin, S. (2018). The Equifax Data Breach: What to Do. Retrieved April 16, 2018, from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

[5] Equifax. (2017). Consumer Notice - Cybersecurity Incident & Important Consumer Information | Equifax. Retrieved April 16, 2018, from https://www.equifaxsecurity2017.com/consumer-notice/

[6] Equifax. (2018). Equifax Releases Updated Information on 2017 Cybersecurity Incident. *Equifax.com.* Retrieved April 15, 2018 from https://investor.equifax.com/news-and-events/news/2018/03-01-2018-140531340