2017 EQUIFAX DATA BREACH

MEDIA CRISIS EVALUATION

PREPARED BY

Rosemarie L. Cordell
COMSTRAT 701, Spring 2022
Washington State University

INTRODUCTION

Equifax is one of three major consumer credit reporting agencies in the United States. The company was founded in 1899 in Georgia by the Woolford brothers, originally compiling customer data by going door-to-door to Atlanta businesses (Reese, 2006). Over 120 years later, the company now serves 13 countries with an estimated $1.4 billion in annual revenue (Reese, 2006). The company has expanded beyond credit investigations and performs a myriad of global data services. According to equifax.com, they aggregate credit and demographic information for businesses, analyze risk, and sell credit monitoring products direct to consumers.

Given the importance of the information Equifax aggregates, they should handle their information with expert care. Unfortunately, Equifax has fallen victim to several hacks, exposing consumer information on the dark web. This case study will assess Equifax's media response to the 2017 data breach, which impacted almost every American over 18. This report will provide an overview of what happened, the company's response, the public's reaction, and the lasting impact of the crisis. Also included is an analysis of where the company misstepped and how they could improve their crisis responses in the future.

EQUIFAX BY THE NUMBERS

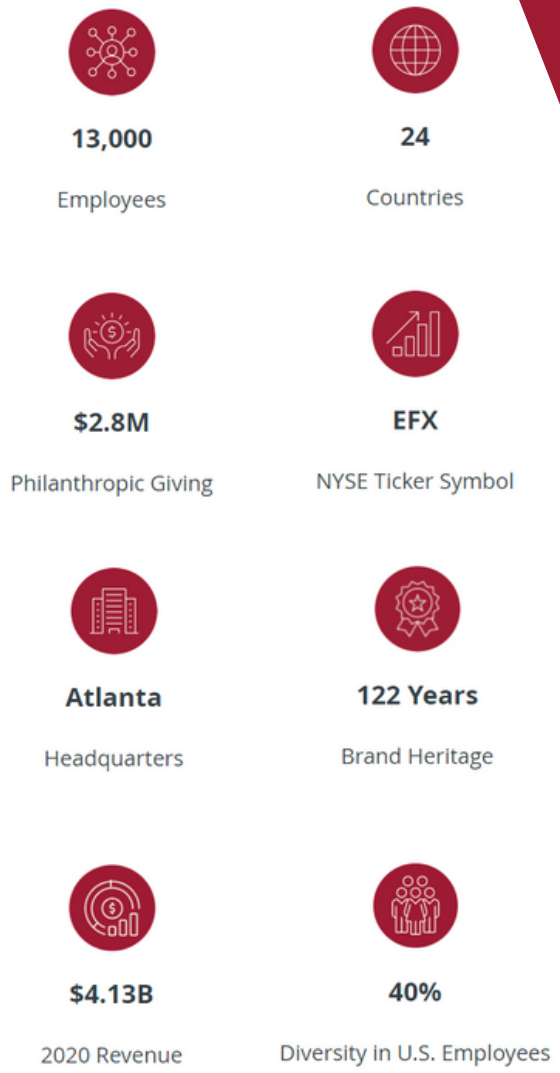

Figure 1 (cover photo) and Figure 2 (this page): from "Equifax: Who are we?" (n.d.)

WHAT HAPPENED?

The 2017 Equifax data breach exposed the personal information of over 140 million people (Federal Trade Commission, 2022). The breach was related to an open-source software called Apache Struts (The Associated Press, n.d.). Apache Struts is a commonly used framework for web-based applications in use by “at least 65% of the Fortune 100 companies” using web applications (Richter, 2020). Like any open-source software, patches are frequently available to address failures or vulnerabilities. A patch for the software was released on March 7, 2017 (Electronic Privacy Information Center, n.d.). The Department of Homeland Security reached out the next day to all three credit bureaus to notify them of the risk and availability of the patch, but Equifax failed to install it right away (Electronic Privacy Information Center, n.d.).

About two months after the release of the vulnerability patch, in May of 2017, hackers started to access Equifax’s computer systems and steal the personal information of everyone in Equifax’s computer system (The Associated Press, n.d.). As a result of this breach, almost every American adult was exposed, increasing the risk of identity theft for the rest of their lives (Novak & Vilceanu, 2019). The timeline below provides an accounting of the events.

2017 DATA BREACH TIMELINE

MARCH

- 7th - The Apache Software Foundation reported the vulnerability and released a patch.
- 8th - Department of Homeland Security contacted Equifax, Experian, and TransUnion to notify them of the vulnerability.
- 9th- An internal email notification was sent to Equifax administrators directing them to patch the Apache vulnerability.
- 15th- Equifax's information security department ran scans meant to identify systems that were vulnerable to the Apache Struts issue, but the scans did not identify the vulnerability

MAY

- May 13, 2017- Hackers began to access personal identifying information.

JULY

- 29th - Equifax discovered “suspicious network traffic” associated with its consumer dispute website. Its information security department applied the Apache patch.
- 30th - Equifax’s information security department observed further suspicious activity and took the web application offline.
- 31st - Equifax’s Chief Information Officer notified CEO Richard Smith of the suspicious activity.

AUGUST

- 1st - Three senior Equifax executives sold stock worth almost $1.8 million.
- 2nd - Equifax hired cybersecurity firm Mandiant to conduct a forensic investigation of the breach.

SEPTEMBER

- 17th - Equifax announced the security breach to the public on Twitter.
- 11th - 20 Senators wrote Equifax a letter asking the company to clarify its position on the Consumer Financial Protection Bureau’s rule.
- 13th - Senator Mark Warner requested an investigation into the breach.
- 14th - Representatives Lamar Smith and Trey Gowdy notify the Equifax CEO that they're opening an investigation into the breach and requesting relevant business records.
- 15th - 2 Equifax executives resigned. Equifax issued a press release confirming that the vulnerability was Apache Struts CVE-2017-5638.
- 27th- Interim CEO published a public apology on behalf of Equifax, and announced a new free service allowing people to lock and unlock their credit.

OCTOBER

- 3rd - IRS awarded multimillion-dollar fraud-prevention contract to Equifax.
- 12th - IRS temporarily suspended its contract with Equifax.
- 12th - Security researchers discovered that Equifax’s website contains false Adobe Flash download links that trick users into downloading malware that displays unwanted ads online.

Figure 3: Adapted from Equifax Data Breach by Electronic Privacy Information Center (n.d.)

EQUIFAX RESPONSE

Equifax executives were initially slow to respond to the crisis in public but did several things behind closed doors. Over the first few months, internal officers and engineers observed suspicious activity and investigated (Electronic Privacy Information Center, n.d.). The Apache patch was finally applied towards the end of July, and the impacted web application was taken offline (Electronic Privacy Information Center, n.d.). During this time, three senior executives also sold off some of their stock in the company, worth almost $2 million (Electronic Privacy Information Center, n.d.).

On September 7th, six months after the initial breach, Equifax finally made an announcement on the company's Twitter feed and released a YouTube video expanding on the incident (Equifax, 2017; Electronic Privacy Information Center, n.d.). These initial communications left out several important facts and pointed users to a separate domain not connected to their parent site, equifaxsecurity2017.com, where potential victims could check their information (Newman, 2017). If the different domain wasn't enough, someone immediately created a spoof site with a similar URL which Equifax later shared on their Twitter site along with a similarly styled phishing link several times, creating public distrust and confusion (Newman, 2017). Eventually, Equifax suspended the company's Twitter account due to the backlash and stopped interacting with the public. Several high-ranking officials left the company shortly after the breach, and a federal investigation ensued.

"EQUIFAX IS OFFERING A FREE COPY OF MY CREDIT REPORT. OF COURSE, APPARENTLY IT WAS ALREADY OFFERING A FREE COPY OF MY CREDIT REPORT"
@INAFRIED

PUBLIC RESPONSE

The public reaction was a mix of fear, anger, frustration, and loss of trust. A poll "conducted by CNN and SSRS found that 72% of Americans voiced concern with both the data breach and Equifax's ability to manage private sensitive data in the future" (Novak & Vilceanu, 2019).

Twitter users began bashing the company on social media. Ina Fried (2017) using handle @inafried commented, "Equifax is offering a free copy of my credit report. Of course, apparently it was already offering a free copy of my credit report." Other Twitter users added hashtags like #Equifail and #WheresMyData to their disgruntled posts (Novak & Vilceanu, 2019).

Two class-action lawsuits were filed by victims in Portland, OR, and Atlanta, GA, which alleged Equifax was negligent in protecting consumer data (Volz & Shephardson, 2017). Several federal agencies held hearings examining the breach resulting in an official Federal Trade Commission investigation (Volz & Shephardson, 2017). A federal court ruled in favor of consumers and issued a settlement resolving the lawsuits.

MIXED MESSAGES

Senator Elizabeth Warren launched an investigation into the Equifax data breach that illuminated several inconsistencies with Equifax's messaging. In early 2018, Warren said in a scathing statement that "[f]or years, Equifax and other big credit reporting agencies have been able to get away with profiting off cheating people, Our report provides answers about what went wrong at Equifax" (Kanell, 2018)

Sen. Warren's report found that not only was consumer information exposed but it was extricated from Equifax's computer system, meaning hackers could retain it for later use (Berry, 2018). Additionally, Equifax failed to notify users that their passport numbers were exposed, along with social security numbers, addresses, and birth dates (Berry, 2018).

Thanks to a federal investigation, we now know that the initial video released by then CEO Rick Smith contained inaccurate information. In the video, Smith said they were made aware of the breach in July, about two months after executives were initially alerted by their internal security team (Equifax, 2017; Electronic Privacy Information Center, n.d.). He also said they acted immediately during the video, which we now know was not the case.

Initially, Equifax told victims there would be a fee to freeze their credit as a preventative measure due to the breach (Volz & Shephardson, 2017). Equifax added language to their relief services, indicating users would be waiving their rights to sue the company if used, but after public backlash, both statements were retracted and revised on their sites (Volz & Shephardson, 2017).

Figure 4: From The Atlanta Journal-Constitution (2018)

> FOR YEARS, EQUIFAX AND OTHER BIG CREDIT REPORTING AGENCIES HAVE BEEN ABLE TO GET AWAY WITH PROFITING OFF CHEATING PEOPLE. OUR REPORT PROVIDES ANSWERS ABOUT WHAT WENT WRONG AT EQUIFAX.

CRISIS PREPAREDNESS

"WHEN YOUR SOCIAL MEDIA PROFILE IS TWEETING OUT A PHISHING LINK, THAT'S BAD NEWS BEARS."
- MICHAEL BOROHOVSKI, TINFOIL SECURITY

By all accounts, Equifax was ill-prepared for a crisis of this nature. The company did well to provide the public with a way to check whether their personal information was exposed. It was also a good idea for the company's social media page to communicate with the public and follow that communication up with a more in-depth video on YouTube. However, they had countless failures that indicated a lack of preparedness. The first was their delayed response. As soon as they discovered the breach, the public should have been notified of the potential risk. Additionally, using a separate domain from their corporate website and charging potential victims a fee to freeze their credit during the crisis damaged the company's credibility in the public eye.

Further evidence of their lack of preparedness was demonstrated when Equifax shared a phishing link four times during the crisis (Newman, 2017). One website security expert summed the situation up with "when your social media profile is tweeting out a phishing link, that's bad news bears" (Newman, 2017). Equifax should have created a subpage on their parent site and provided free support, which would have provided some inherent trust. They should have also had someone checking their Twitter posts to ensure correctness.

Figure 5: From Equifax "Who are we?" (n.d.)

EVIDENCE OF IMPACT

Everyone in Equifax's database will be at risk for identity theft for the rest of their lives. Unfortunately for many, the best option is to monitor their credit regularly for signs of theft or put a freeze on their credit to prevent their information from being used. Thanks to the class-action lawsuit, Equifax will have to pay up to $425 million to help people affected by the data breach (Federal Trade Commission, 2019). The settlement includes free credit monitoring to those impacted for up to 10 years, along with identity restoration services if you become the victim of theft or fraud (Federal Trade Commission, 2019).

The infographic below can be found on the Federal Trade Commission's website and is a helpful guide on what to do if your information is stolen.

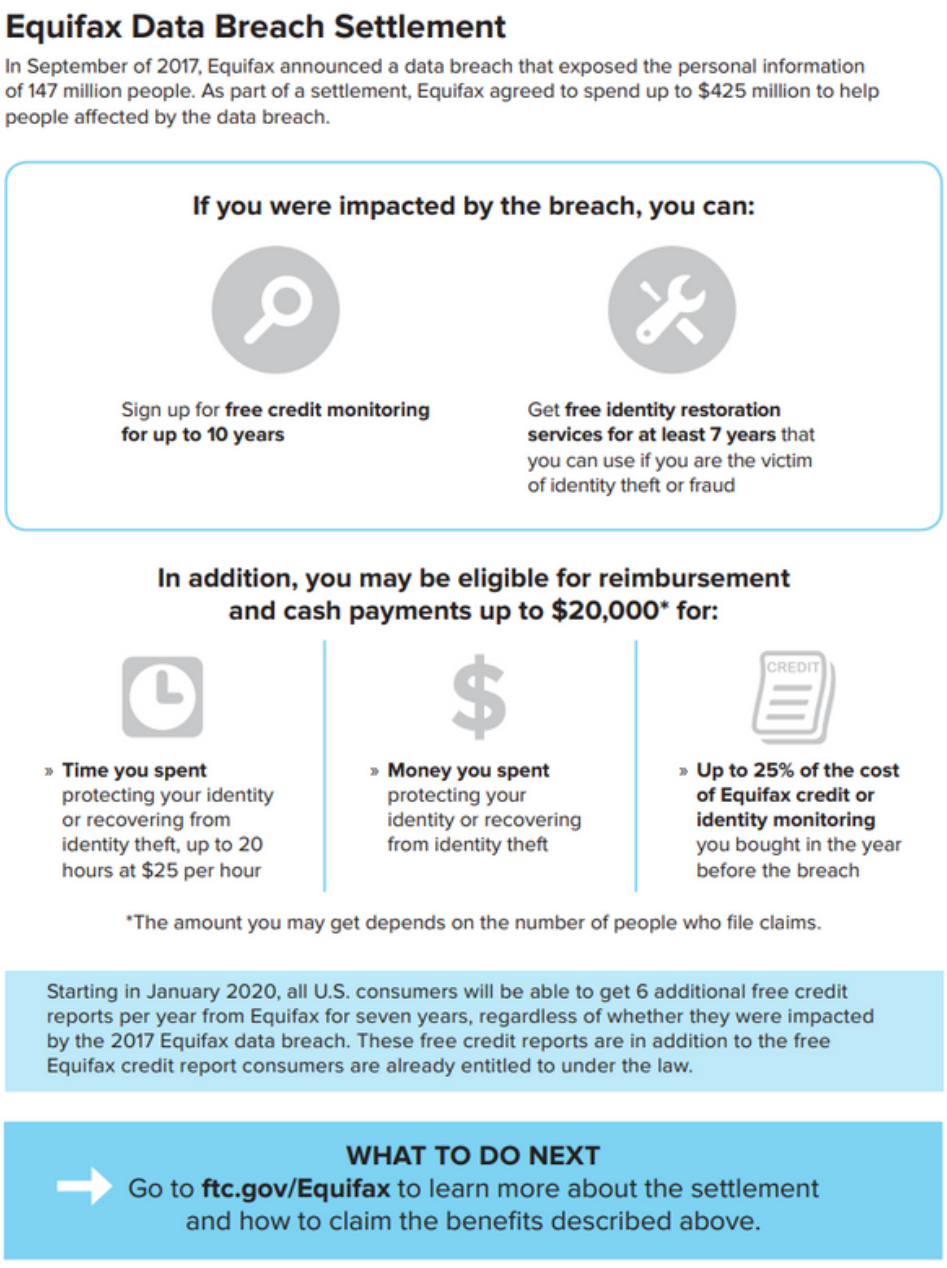

Figure 6: From Federal Trade Commission (2019)

LESSONS LEARNED

"EQUIFAX SITS ON THE CROWN JEWELS OF WHAT WE CONSIDER PERSONALLY IDENTIFYING INFORMATION" - JASON GLASSBERG,

From a crisis response perspective, it's easy to learn lessons from the Equifax data breach because it's clear that the company was ill-prepared for this crisis. Having a plan before a crisis occurs is an essential first step. A crisis communication plan would provide instructions for how and when to respond to the public. A plan would also outline the different types of crises a company may face and who should be pulled in to advise and at what time.

Jason Glassberg, the co-founder of the corporate security and penetration testing firm Casaba Security, said that "Equifax sits on the crown jewels of what we consider personally identifying information," and "you'd think a company like that, guarding what they're guarding, would have a heightened sense of awareness and that clearly was not the case." (Newman, 2017). Companies using public-facing applications or managing personally identifiable information should have security protocols in place to mitigate risk. In the future, Equifax's security engineers should have an established timeframe they stick to for testing and releasing software patches and a risk mitigation plan for issues when they arise.

CONCLUSION

Today, there is almost no mention of the 2017 data breach on Equifax's website. The company website now features robust messaging around its data security and new policies. Equifax has rebranded and refocused its messaging. However, the victims involved are still living with the consequences. Fortunately, there is help in the form of credit monitoring and restoration services, thanks to the Federal Trade Commission and the many class-action lawsuits across the country.

Thanks to this data breach, there is increased scrutiny on all three major credit bureaus, and further legislation is being pursued to keep things in line in several different federal offices. This case study should be considered a warning to unprepared companies thinking of winging it during a crisis. Companies should have a plan in place along with a mitigation strategy for when things go wrong. Regardless, transparency, authenticity, and timeliness are essential to successful crisis communication, regardless of the situation.

REFERENCES

Berry, K. (2018). Equifax misled public on data breach, Warren claims. *American Banker, 183*(27), 1.

Electronic Privacy Information Center. (n.d.). *Equifax data breach.* https://archive.epic.org/privacy/data-breach/equifax/

Equifax. (2017, September 7). *Rick Smith, chairman and ceo of Equifax, on cybersecurity incident involving consumer data* [Video]. Streaming Service. https://www.youtube.com/watch?v=bh1gzJFVFLc

Equifax. (n.d.). *Who are we?* About Equifax. https://www.equifax.com/about-equifax/who-we-are/

Federal Trade Commission. (2022). *Equifax data breach settlement.* Refunds. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

Fried, I. [@inafried] (2017, September 7). *Equifax is offering a free copy of my credit report. Of course, apparently it was already offering a free copy*[Tweet]. Twitter. https://twitter.com/inafried/status/905922850216964097?ref_src=twsrc%5Etfw

Kanell, M.E. (2018, February 8). *Equifax lambasted again in a new senate report.* The Atlanta Journal-Constitution. https://www.ajc.com/business/equifax-lambasted-again-new-senate-report/SsfDDTy0vObqvLiEN4FcFJ/

Reese, K. (2006). Equifax. In *New Georgia Encyclopedia*. https://nge-staging-wp.galileo.usg.edu/articles/business-economy/equifax/

Newman, L. H. (2017, September 24). *All the ways Equifax epically bungled its breach response.* Wired. https://www.wired.com/story/equifax-breach-response/

Novak, A. N., & Vilceanu, M. O. (2019). The internet is not pleased: Twitter and the 2017 Equifax data breach. *The Communication Review, 22*(3), 196-211. https://doi.org/10.1080/10714421.2019.1651595

Richter, A. (2020, November 22). *Apache Struts vulnerabilities pose 'stay or go' question.* White Source. https://www.whitesourcesoftware.com/resources/blog/apache-struts-vulnerabilities/

The Associated Press. (n.d.). Equifax CEO retires in the wake of damaging data breach. *Long Island Business News (Ronkonkoma, NY).*

Volz, D., & Shepardson, D. (2017, September 8). *Criticism of Equifax data breach response mounts, shares tumble.* Reuters. https://www.reuters.com/article/us-equifax-cyber/criticism-of-equifax-data-breach-response-mounts-shares-tumble-idUSKCN1BJ1NF