2018

Equifax: Anatomy of a Security Breach

Ashton Glenn
Georgia Southern University

Equifax: Anatomy of a Security Breach

An Honors Thesis submitted in partial fulfillment of the requirements for Honors in the College of Business Administration, School of Accountancy.

By
Ashton Glenn

Under the mentorship of Dr. Thomas Buckhoff

ABSTRACT

The infamous 2017 Equifax breach not only compromised millions of citizens' data, but the breach also left Equifax vulnerable to lawsuits that claim the company acted negligently. This thesis analyzes the events and facts behind the incident to determine the probable outcome of the main case against Equifax. A claim of a breach can come from either Equifax's data protection or breach response. This thesis concludes the results of the case depends on the final court to determine if Equifax acted negligently with its data protection. If the case ends in the Eleventh District Court of Appeals, the court will probably decide Equifax was negligent. If the case ends in the Supreme Court, the Court will probably decide Equifax was not negligent. This thesis also concludes that Equifax did not act negligently with its response to the breach.

Thesis Mentor:_____

Dr. Thomas Buckhoff

Honors Director:_____

Dr. Steven Engel

November 2018
School of Accountancy
University Honors Program
Georgia Southern University

Acknowledgments

I would like to thank the School of Accountancy faculty and the University Honors Program for supporting me throughout my thesis and academic career. I would especially like to thank Dr. Thomas Buckhoff, my faculty mentor, for guiding me along my thesis journey. His knowledge and insights were indispensable for the completion of this thesis. I would also like to thank my friends and family for constantly encouraging me to work hard and do my best.

Introduction

The collection and use of data have quickly become a vital part of the business world with terms such as "Big Data" dominating corporate philosophy. This trend unfortunately also brings a heavy repercussion to many citizens. Multiple data breaches occur each year that compromise people's financial information. An identity theft brought on from a data breach can cost hundreds of hours and thousands of dollars to resolve (Synovate, 2017). This thesis examines if Equifax acted negligently with the company's data protection and breach response during the 2017 data breach. Negligence is defined as "A failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances. The behavior usually consists of actions, but can also consist of omissions when there is some duty to act" (Legal Information Institute, 2017). To determine if Equifax was negligent, the thesis will examine 1) if Equifax has a duty to protect data and notify breach victims and 2) if Equifax does have a duty, did Equifax breach one or both duties with their actions or lack of actions. Fully understanding the issue requires a base level of knowledge of the following concepts.

Consumer Reporting Agency

A consumer reporting agency (CRA), also known as a credit reporting agency or credit bureau, collects individuals' financial information to generate financial reports. Three major CRAs exist in the United States: Experian, TransUnion, and Equifax. The reports generated by the CRAs provide the information behind FICO® Scores which rate individuals on their credit worthiness. CRAs normally sell these reports to banks, lenders, and other business for various reasons. The US government doesn't directly own or

control any CRAs, but Congress has enacted laws concerning CRAs' operations. The Federal Trade Commission (FTC) has oversight over CRAs to ensure compliance with these laws and regulations.

Equifax Data Breach

The following bullet point list represents the simplified and condensed version of the series of events that lead to the breach according to the former CEO of Equifax (Smith, 2017). Even though the statement comes from the culpable party, this source provides the most detailed and extensive account of the situation. The United States Government Accountability Office has verified multiple events in its report which lends further credibility to the testimony (2018). Some additional details have been added from Smith's other statements from the same hearing or from other sources.

- March 8, 2017: Homeland security issued a notice to multiple companies about a vulnerability for the software "Apache Struts." The software developer released the associated patch along with the announcement. Equifax used this software in one of Equifax's main claims dispute websites.
- March 9: Equifax sent an email to security personnel to update the software in accordance with their 48-hour policy. Equifax staff failed to update the software because a sole employee forgot to implement the update.
- March 15: Equifax information system scans failed to detect the vulnerability in any of the software.
- May 13: The first known date that the hackers probably accessed sensitive information exploiting the vulnerability. This access probably continued until July

30, 2017. During this time period, none of Equifax's security measures detected the breach.

- July 29: Equifax security department detected suspicious activity with the website, so security blocked the source.
- July 30: Equifax security found more suspicious activity, so security shut down the website.
- August 2: Following internal procedures, Equifax hired a law firm for legal advice, hired a forensic consulting firm to investigate, and notified the Federal Bureau of Investigation (FBI). The FBI did not start an investigation yet.
- August 11: Equifax's internal investigation found that the hackers had access to consumers' sensitive information.
- August 15: The sensitive information had been confirmed as stolen. The investigation continued to determine the scope of the breach.
- September 4: The investigation created a list of 143 million people believed to have had their personal information stolen. Equifax notified the FBI about the upcoming planned press release.
- September 7: Equifax released a press release announcing that the breach impacted personal information relating to 143 million U.S. consumers. The stolen information mostly consisted of names, Social Security numbers, birth dates, addresses, and driver's license numbers.
- September 18: The FBI launched a criminal investigation intended to examine multiple aspects of the incident (Viswanatha & Kendall, 2017).

- December 6: The U.S. Judicial Panel on Multidistrict Litigation transferred hundreds of cases from every state to Atlanta, Georgia to consolidate all the individual cases into one case (McDonald, 2017). The cases will be tried at the United States District Court for the Northern District of Georgia which is under the United States Court of Appeals for the Eleventh Circuit (McDonald, 2017).

Negligence

Most plaintiffs use the negligence statute when they want to sue a company for harm that they have received. The main manner to assess negligence is by using the reasonable person test. The test asks, "Would a reasonable person have acted the same as the defendant with normal foreseeable circumstances and consequences?" Negligence can involve either improper actions or inactions when an entity had a duty to act. According to the Legal Information Institute, to consider an entity's actions as professionally negligent, each of these four elements must stand true:

1. the existence of a legal duty that the defendant owed to the plaintiff
2. defendant's breach of that duty
3. plaintiff's sufferance of an injury
4. proof that defendant's breach caused the injury

Body

Data Protection

1. Existence of Duty

In general, a person doesn't need to help or protect someone. This fact changes when there exists a legal relationship between the parties or when the defendant acted unlike a reasonable person. For example, if someone is drowning in a pool, a passerby has no obligation to save that person despite how negatively society might view the passerby. However, if there is a lifeguard on duty, the lifeguard has a duty to save the person because saving a drowning person is a part of the lifeguard's job. A relevant question to ask is "Does a legal relationship exists between Equifax and the common consumer?" Even though Equifax has not created a contract with every consumer or even directly contacted each consumer, Equifax established a relationship when the company started to collect consumers' private information.

Equifax places consumers in excess danger since the information Equifax collects can cause damages to a consumer if the information gets in harm's way. Since Equifax creates additional danger, Equifax must protect consumers from the foreseeable risks associated with collecting data. Even though Equifax is not a person, the company still needs to perform in a way that an entity in a similar position should and normally does act. This form of "reasonable person" is called the professional standard of care. In this instance, a responsible company must establish and maintain controls to protect data. A reasonable company recognizes the harm that can come from an outsider obtaining private information.

The importance to protect sensitive information is especially high for an online access point to a database. Databases have more vulnerabilities when they are connected to the internet. Online access points serve as easily accessible places hackers choose to attack. Since online access points will receive the most attacks, companies need to implement more protections to guard these points of attack. Since Equifax endangered sensitive information by placing the information in a vulnerable location, Equifax owed a duty to consumers to protect their sensitive information.

2. Breach of Duty

To protect the data Equifax had collected, Equifax needed to have sufficient protections and procedures in place. Equifax failed this duty in three areas:

- Maintaining Policy
- Proper Software Audits and Checks
- Backups and Redundancies

Maintaining Policy

Even though Equifax recognized the threat of a breach and implemented a corporate policy for protection (Equifax Inc., n.d), Equifax's IT failed to protect the system with important software updates. A policy of protection serves no purpose if the company doesn't properly follow the policy. Even if a company has properly designed controls, the company has no protections at all if the employees fail to follow prescribed procedures. The success or failure of a major portion of a company's system should not rely solely on one employee like in the Equifax breach. Equifax also did not perform management checks that Equifax claims on the company's website (Equifax Inc., n.d).

Proper Software Audits and Checks

Equifax conducted a software audit that failed to detect any weaknesses in the software. Presumably, Equifax's staff neither properly designed nor conducted the audit since the staff failed to detect the website weakness which was the audit's sole purpose. A check doesn't need to be technical, a simple check could come from a supervisorial review of the employee's work. Equifax not only failed to detect the online portal weakness on just one occasion, but also for an extended period of time. A company doesn't need to have a full system audit every day or look at each piece of data, but a company should at least have the individual controls in place that can detect any outdated software or unusual events.

Backups and Redundancies

In general, Equifax had too much confidence that the system was invulnerable to any major errors or attacks. This false confidence caused Equifax to not create any extra checks or redundancies. The word redundancy often carries a negative connotation, but a redundancy provides more security in the field of information system design. If one level of security fails, redundancies back up the function and prevent total failure. The company who developed the website software stated as much in a press release, "It is good software engineering practice to have individually secured layers behind a public-facing presentation layer such as the Apache Struts framework. A breach into the presentation layer should never empower access to significant or even all back-end information resources" (The Apache Software Foundation, 2017). A more drastic example of the importance of redundancies comes from nuclear weapons. No nation would have total trust with only one mechanism to prevent accidental detonation. The

extra protection doesn't have to cost more than the additional benefits, but one extra layer of software protection could have prevented this incident.

3. and 4. Damages

For this thesis, the third and fourth elements have been combined because they both involve a legal grey area. There currently exists a divide in the American courts as to whether future damages from a data breach allow enough standing for a breach of duty (Mank, 2017). On one side of the issue, most appellate courts have ruled that the damages must have already occurred to have a standing (Mank, 2017). On the other side, some appellate courts have ruled that there exists a standing if the actions caused "substantial risk" (Mank, 2017). An example of this contention comes from Clapper v. Amnesty International USA where the Supreme Court decided that the future damages of compromised data in the case were too speculative. In the case's ruling, the Supreme Court did acknowledge that the substantial risk test has been used in prior cases. The results of the Equifax case will most likely depend on where the case will end.

In the Appellate Court

If the case ends in the Eleventh District Court of Appeals, the court will probably apply the substantial risk test. The Eleventh District Court of Appeals has already favored a more liberal view in favor of the plaintiff in Curry, et al. v. AvMed, Inc. Under the substantial risk test, the court will decide that the future harm provides enough standing for the third and fourth elements of fraud. The theft of data from a database provides substantial risk of future harm. The main reason hackers take data from servers is to steal

the identity of the victims or to sell the information to others. Both situations will bring probable damages to the victims of the Equifax breach.

In the Supreme Court

The issue of whether the Supreme Court will take up this case remains unclear. The Supreme Court has already denied a request to review a data breach case with Attias v. CareFirst (Shepard, 2018), but the size and importance of the Equifax breach may push the Supreme Court to accept this case. If the Supreme Court accepts the case, the Court will probably utilize a stricter standard to decide the case. The current Supreme Court tends to favor businesses more than consumers in the Court's most recent decisions (Epstein et al., 2017). Under the stricter standard, the future harm will not suffice as standing for damages. The conservative leaning Supreme Court may use this decision to urge for Congress to implement a law to punish poor data protection, but the Supreme Court will probably not venture outside the traditional interpretation of the elements. The original interpretation requires damages to have already occurred and be provable. Most of the damages have not occurred yet and there is no way to prove the hackers have already exploited most of the data for nefarious purposes.

Breach Response

1. Existence of Duty

Equifax needed to notify the public about the data breach in a timely manner since time can be an important factor with mitigating damages. Victims of data breaches often can mitigate the damages when they become aware of the data breach. The longer a fraud

lasts, the more overall value stolen and out of pocket expenses increase. The following passage from a report commissioned by the FTC illustrates this fact:

> "When the misuse was discovered within 5 months of the initial misuse, the value obtained by the thief was $5,000 or more in only 11% of the cases. Where discovery took 6 months or more, the value obtained by the thief was at least $5,000 in 44% of cases. . . Victims who quickly discovered that their information was being misused were less likely to incur out-of-pocket expenses. No out-of-pocket expenses were incurred by 67% of those who discovered the misuse less than 6 months after the misuse began. Only 40% of victims who took 6 months or longer to discover the misuse were able to avoid incurring some such expenses." (Synovate, 2017, p. 41-44)

Since Equifax has direct control of when the consumer becomes aware of the situation, Equifax is also responsible for any additional damages incurred by the consumer. Equifax can mitigate additional damages if Equifax responds in a timely manner as a responsible company. The FTC has even published a guideline called "Data Breach Response: A Guide for Business" so that businesses will know the best way to respond when they experience a breach.

2. Breach of Duty

"Data Breach Response: A Guide for Business" by the FTC serves as a good template for how Equifax should have responded. Even though this guideline has no direct legal binding statutes, the guideline establishes standards that a reasonable company should follow after a breach. The applicable sections for this guide are the

responsibility of securing operations and notifying appropriate parties. In general, Equifax stuck fairly close to the suggested actions.

Securing Operations

The first prescribed action is to contact legal counsel and data forensic experts. Equifax did so within the first couple of days even before Equifax knew how serious the data breach was. Equifax responded prudently as the company allowed the data investigation experts to inspect the issue instead of putting an in-house IT professional in charge. One of the most important actions for securing operations involves stopping the data leak when discovered. Equifax shut down the website early on when security first discovered the security breach.

Notifying Appropriate Parties

After a company secures operations and collects the majority of the facts, the company should adequately notify the appropriate parties. A company should first notify appropriate law enforcement to ensure a proper investigation of the issue. Equifax did so by contacting the FBI when Equifax first discovered the breach. Equifax hasn't specifically disclosed if the company notified all state authorities, but Equifax probably did because no state governmental claims have come to light. The most important entity to notify is the consumers who had their data exposed. The notification should not only let the consumers know they are vulnerable, but the notifications should also fully and clearly describe what the company knows about the situation. In Equifax's press release, Equifax described how the incident occurred, what information was taken, and what actions they have taken to remedy the situation (Equifax, 2017).

Small Area of Vulnerability

The only area that makes Equifax vulnerable to a standing of a breach of duty comes from Equifax's mishandling of the online breach help resources. To help consumers find out if they were compromised, Equifax set up a website to allow consumers to check their statuses. The problem with the help resources comes from how little effort Equifax put behind the website and the accompanying hotline. An example of incidents includes people not receiving a requested response or the resources not working because of an influx of traffic (Singletary, 2017). This delay effectively caused the majority of consumers to not receive the breach notification till weeks later. An influx of traffic is normal when consumers learn of an unexpected security breach, but Equifax had around a month to fully prepare all the systems for the foreseeable new traffic. Since Equifax did not properly prepare its resources, it may still be vulnerable to a standing.

3. and 4. Damage

For the majority of the victims of the data breach, they were not significantly damaged in the one-month period between discovery and notification. The hackers couldn't fully capitalize on all the information collected during the short period of time. The plaintiffs would struggle to demonstrate that the majority of the victims will experience increased damages between discovery and notification. The main harm of a data breach doesn't come from the immediate impact, but from the lifelong harm of compromised sensitive information. The third and fourth elements of negligence will not have sufficient standing using either the substantial risk test or the traditional test.

Conclusion

Data Protection

Equifax had a legal duty to protect consumers' data and breached that duty by allowing weaknesses and failing to detect the breach. Whether the plaintiffs suffered damages and if Equifax's breach caused the damages depends on the interpretation by the final court. If the Eleventh District Court of Appeals has the final decision, the court will probably decide Equifax caused damages so Equifax was negligent. If the Supreme Court has the final decision, the court will probably decide Equifax did not cause damages so Equifax was not negligent.

Breach Response

Equifax had a legal duty to respond in an appropriate manner to a data breach. Equifax did not breach their duty to respond to the data breach, the plaintiffs did not suffer damages from the response, and Equifax's breach did not cause the damages. Therefore, Equifax was not negligent with the company's breach response.

Reference

The Apache Software Foundation. (2017, September 9). Apache Struts Statement on Equifax Security Breach. Retrieved from https://blogs.apache.org/foundation/date/20170909

Bernard, T. S. (2017, September 18). Prosecutors Open Criminal Investigation into Equifax Breach. Retrieved from https://www.nytimes.com/2017/09/18/business/equifax-breach-federal-investigation.html

Clapper v. Amnesty International, 568 U.S. 398 (2013)

Curry, et al. v. AvMed, Inc., No. 11-13694 (11th Cir. 2012)

Epstein, Landes, & Posner. (2017). When It Comes to Business, the Right and Left Sides of the Court Agree. W*ashington University Journal of Law & Public Policy.* 54, 33-55. Retrieved from http://epstein.wustl.edu/research/businessSupCtUpdate.html

Equifax Inc. (n.d.). Security. Retrieved from https://www.equifax.com/eport/security//

Equifax Inc. (2017, September 7). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved from https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Federal Trade Commission. (2016, September). Data Breach Response: A Guide for Business. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

Legal Information Institute. (2017, June 06). Negligence. Retrieved September 15, 2018, from https://www.law.cornell.edu/wex/negligence

Mank, B. (2017, January). Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits? *Notre Dame Law Review*, 92(3), 1323-1367. Retrieved from https://scholarship.law.nd.edu/ndlr/vol92/iss3/7/

McDonald, R. R. (2017, December 07). Judicial Panel Orders Equifax Data Breach Cases Consolidated in Atlanta. Retrieved from https://www.law.com/dailyreportonline/sites/dailyreportonline/2017/12/07/judicial-panel-orders-equifax-data-breach-cases-consolidated-in-atlanta/

Shepard, K. (2018, February 21). Supreme Court Declines Review of Standing in Data Breach Class Actions. Retrieved from https://www.jdsupra.com/legalnews/supreme-court-declines-review-of-44991/

Singletary, M. (2017, September 19). Equifax says it's overwhelmed. Its customers say they are getting the runaround. Retrieved from https://www.washingtonpost.com/news/get-there/wp/2017/09/19/equifax-says-its-overwhelmed-its-customers-say-they-are-getting-the-runaround/?utm_term=.51e30f73f767

Smith, R. (2017). Prepared Testimony of Richard F. Smith before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection. Retrieved from

https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf

Synovate (2003, September). Federal Trade Commission–Identity Theft Survey Report. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-identity-theft-program/synovatereport.pdf

United States Government Accountability Office (2018, August). Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. Retrieved from https://www.gao.gov/assets/700/694158.pdf

Viswanatha, A., & Kendall, B. (2017, September 08). FBI Looking into Equifax Data Breach. Retrieved from https://www.wsj.com/articles/fbi-looking-into-equifax-data-breach-1504902745