O

by S N

Submission date: 26-Jun-2021 04:36AM (UTC-0500)
Submission ID: 1612372395
File name: The_Legal_Issue_in_Equifax_Data_Breach.edited.docx (20.86K)
Word count: 1616
Character count: 9137

The Legal Issue in Equifax Data Breach

Name:

Institution:

Course:

Instructor:

Date:

The Legal Issue in Equifax Data Breach

When it comes to implications and legal ramifications, security breaches can be devastating. When an agency like Equifax with massive power and access to millions of clients' details is breached, the gravity of the situation only grows. A customer data leak in which personal information about the customers is divulged is even more catastrophic. While it is evident that extra efforts should be made to prevent cyber-attacks, the reality is that security breaches will inevitably occur owing to the constantly increasing rate of incidents and the ever-growing technological environment. According to retired Federal Bureau of Investigation Director Robert Mueller, there exist two kinds of organizations: those that have been breached and others that will be attacked. In addition to that, companies that have been hacked are likely to be hacked again. This paper aims to discuss the legal issue surrounding the Equifax data breach.

In a credit consumer bureau scenario, where the possible liability is significant, the critical question is: what is the appropriate legal redress for acquiring appropriate compensation when a breach has occurred? This problem arose after Equifax, one of the most extensive consumer credit programs in the United States, disclosed a massive cyber-attack within its online network (FEDERAL TRADE COMMISSION, 2019). As a result, the data breach revealed the confidential material of roughly 145 million customers. Of course, resolving data breaches is not new, and it gives many challenges to the legal profession. Nevertheless, with a transition toward increased consumer safety and a fundamental dedication to concurrently safeguard and enhance business growth, the issue of which aspects of judicial redress, litigation, arbitration, or an institutional remedy, should reign supreme to achieve such ends persists.

While technological innovations can provide substantial advantages to the target audience, they can also cause severe damage. Today, we live in a “big data” world. The majority of customers use card payments, and private information is shared on online platforms daily. While this implementation of technology is unquestionably beneficial, the world today amplifies the vulnerability of sensitive consumer data. A data breach is defined as unauthorized access to personal data. An event where an entity's identity plus Social Security Number (SSN), health or banking record, driver's license, credit or debit card is presumably at risk, whether in electronic or printed format. Regrettably, professional hackers, who are frequently the perpetrators of data breaches, are highly advanced in using technological advancements to collect information and then sell it on the dark web. As a result, cyber-attacks are increasing in both frequency and intensity. Despite increased regulatory oversight and increased information security expenditure, the number of incidents has increased. As per the FEDERAL TRADE COMMISSION (2019) report, the number of American cyber-attacks tracked into June 30, 2017, hit a half-year shows a high of 791. It shows a significant increase of 29% over 2016 statistics for an exact time frame. They have grown in size in addition to increasing in speed.

As privacy violations continue to increase in the modern, technologically advanced society, the issue of legal recourse has become increasingly important. Reactions to recent data infringements show that there are numerous avenues for redress. Many other major firms, including Home Depot, Target, and eBay, have continued to suffer security breaches in which customers' details have been inappropriately exposed. Customers who have entrusted with a business in exchange for the services (for example, a credit card issuer or financial institution) and confidential data are illegally acquired due to a security breach typically come forward. Companies have tried to avoid litigation by including binding arbitration clauses in their

agreements with customers to fix these civil disputes. Consumers are required by these contracts to resolve any disputes they have with the company via mediation, in which a neutral party decides on the particular issue, instead of going to trial or participating in a civil suit.

I support the position of the article for various reasons and agree with the outcome of the settlement. In general, a person is not required to assist or defend another. Regardless, this fact changes when the entities have a contractual relationship or when the victim acted unreasonably. For instance, if somebody is sinking in a pool, a bystander has no moral responsibility to save that individual, regardless of how adversely society views the bystander. Nevertheless, if a lifeguard is on duties and responsibilities, the lifeguard is obligated to save the individual since saving a drowning man is an aspect of the lifeguard's profession.

A pertinent question to consider is whether Equifax and the average client have a formal contract. Although Equifax has not created a service agreement with each client or even directly contacted each customer, the firm formed a relationship when collecting consumers' data. Based on the article, the FEDERAL TRADE COMMISSION (2019) argues that Equifax has a duty and responsibility to its clients to ensure that their personal information does not get into the wrong hands. Equifax puts people in jeopardy because the data it collects can risk clients if it falls into the wrong hands. Equifax must offer protection from the possible risks related to data collection because it establishes additional risks. Although Equifax is not an individual, the business must act like a person in a comparable predicament should and usually does. The professional level of care refers to this type of "rational person." In this case, a reputable company must create and sustain data protection restrictions. A good company should recognize the potential harm that can result from an outsider acquiring private information.

The company was also criminally liable because of the breach of duty. Equifax needed adequate safeguards and procedures in place to protect the data it had collected. Equifax failed to fulfill this obligation in three significant ways: policy upkeep, proper technology monitors and inspections, redundancies, and data backup (FEDERAL TRADE COMMISSION, 2019). Even though Equifax identified the danger of a breach and enforced a company policy to protect itself, Equifax's information system could not provide critical software upgrades to offer protection. A protection policy is useless if the company fails to implement it appropriately. Even if a company has appropriately implemented safeguards, it has no security if workers refuse to obey guiding principles and practices. Equifax was overconfident that the platform was impervious to critical flaws or threats. Due to this misplaced hope, Equifax did not implement any extra tests or redundancies. In the area of information system development, redundancy offers extra security. When one security level stops working, redundancies take over and help stop a complete disaster. In a public statement, the company that created the web page software asserted that it is a good software engineering strategy to have independently protected sections behind a customer-facing user interface, which the company lacked. In this regard, the criminal lawsuit and the settlement are valid, based on the company's failure to protect consumer data.

If this matter happened to my business, I would make specific changes. For instance, I will install the necessary updates and security patches to my information technology system. In the case of Equifax, initial reports suggest that the vulnerability that hackers saw was the use of an unpatched free version of a web application program (FEDERAL TRADE COMMISSION, 2019). Based on this issue, I find it essential to install the latest security and updates readily offered by the technology firms to protect against vulnerabilities. In addition to that, instead of a class-action suit, I will opt for arbitration that has numerous benefits. For instance, arbitration is

a means of resolving disputes that, compared to conventional class actions, aim to assist consumers and businesses in saving time and resources while achieving good results. Arbitration provides a fast, effective dispute resolution mechanism for both consumers and enterprises as contrasted with more prolonged court action. In addition, arbitration removes the problem of civil suit litigation, in which attorneys file presumably spurious claims with the knowledge that the case has a high chance of being settled.

Also, I would create a client compensation program. Creating a compensation scheme would help compensate victims while reducing the time and resources associated with meritless or under-compensated civil suits. The advantage of a controlled compensation method exceeds the value of private lawsuits since the fund can be set up to make payment quicker and easier. Who can and cannot reclaim and how much they can regain can be more concise and less contentious when an appropriate compensation plan exists. Furthermore, both companies and complainants gain from the surety and sustainability provided by a compensation plan.

To sum it up, I agree with the decision to compensate the victims of Equifax's data breach. The company failed in numerous aspects to protect consumer personal information against unauthorized access, and they are criminally liable. However, the $575 million in compensation is not enough, especially when the victims do not know what was done with their data. In this regard, Equifax must adopt a comprehensive information security strategy to protect it against future breaches. Furthermore, the business should be severe about annual assessments regarding the threats it faces and implement safeguards that address the possible risks like remediation policies, patch systems, and intrusion detection tools. More importantly, Equifax should ensure that they continuously test and monitor their security policies to ensure they are

current. Moreover, rally their service providers who can access the data they store and adopt similar information security mechanisms to avoid lawsuits and criminal liability in the future.

Reference

FEDERAL TRADE COMMISSION. (2019, July 31). *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/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

O

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		