

Equifax's Breach of Trust

Equifax is one of three major consumer credit reporting agencies in the United States. On September 7, 2017, the company announced a cybersecurity data breach that exposed the information of more than 143 million consumers in the United States, approximately 44 percent of the population. The breach occurred because of a vulnerability on Equifax's website. Hackers were able to obtain names, birth dates, addresses, driver license numbers, Social Security numbers, and some credit card numbers, putting many people at risk of identity theft. Equifax officials became aware of the hack on July 29, 2017, more than a month before they let consumers know. The company reported that unauthorized access happened from mid-May through July.

This was not the first time Equifax faced hacking due to flaws in the company's security. Earlier, in March 2017, Equifax faced a separate breach. In this instance the company notified a small number of banking customers and brought in a security firm to assist its investigation into the breach. While this was not made public by Equifax, it did not find evidence that data had been accessed or stolen. Earlier still, in December 2016, a security researcher examined Equifax's servers and alerted the company that its system was vulnerable to the kind of hack that occurred in 2017. Equifax eventually patched this vulnerability, but only after the mid-2017 breach had taken place. Upon investigation by an independent cybersecurity team after the mid-2017 breach, other security flaws were also found.

Journalist Stephen Gandel detailed Equifax's process to verify that consumer data was compromised. After the discovery on July 29 it was not until two weeks later that the company's team of 225 cybersecurity experts could report to the CEO that the firm had been hacked. It was another two days before Equifax was certain that consumer data was compromised. Five days later, Equifax's board was notified. More than two more weeks went by before the security breach was made known publicly. Gandel wrote, "It's important to understand that what happened at Equifax was not just a technological failure but more important a failure of management and corporate governance."

Soon after the data breach was announced in September 2017, reporters discovered that four senior executives at Equifax sold shares of company stock worth nearly \$1.8 million in the days after the July 29 discovery of the breach. Equifax conducted its own investigation and concluded that none of these executives knew of the breach at the time they sold stock. Another executive, however, chief information officer Jun Ying, sold nearly \$1 million worth of stock only days before the breach was publicly announced on September 7. On September 8, Equifax shares fell 14 percent.



Ying avoided more than \$117,000 in losses that he would have sustained had he sold after the disclosure.

After the announcement of the hack, Equifax directed consumers to a website where they could check if their data had been compromised. Users had to submit their last name and the last several digits of their Social Security number. Users also had to check a box in agreement of Equifax's terms of service. These terms included a hidden clause that use of the site waived a user's rights to a class-action lawsuit.

In September 2017, the Consumer Financial Protection Bureau opened an investigation into the data breach on behalf of consumers. A change in leadership at the Bureau stalled investigations, and as of April 2018, further actions have not been taken. In March 2018, the Securities and Exchange Commission filed criminal charges of insider trading against Ying.

Concept: Loss Aversion

Ethical Insight:

People tend to dislike losses more than they enjoy gains and will take greater risks to avoid a loss than to achieve a gain. This seems particularly true when people make a mistake. Often the mistake is one of mere carelessness, yet if the mistake becomes known it can cost people their reputation, their job, even their freedom. To avoid sustaining those losses, people will often cover up the mistake and its consequences, sometimes by actively lying.

When Equifax was hacked and suffered a data breach that compromised the information of nearly half of the American population, that was bad. It showed incompetence on Equifax's part. But Equifax failed to own up to its mistake and intentionally hid the breach. Rather than notify consumers immediately that their personal information may have been affected, company leaders took about six weeks to notify the public. Ironically, instead of avoiding the damage to its reputation, Equifax's failure to own its mistake simply compounded the company's problems.

Discussion Questions:

1. In what ways did Equifax demonstrate loss aversion? Explain.
2. Journalist Stephen Gandel found that several weeks passed before Equifax notified consumers of the security breach. Part of this time was spent verifying that data had been stolen, and then more time passed before the company notified the public. Why do you think the company took this long? Do you think the company was being cautious to accurately assess the situation, or were they trying to cover up their mistakes? Explain.
3. While the mid-2017 security breach was the largest at Equifax, it was not their first. Why do you think the company did not take greater measures to secure their data after

previous breaches? If you were an Equifax executive, what would you have done when you learned of the breach?

4. Do you think Jun Ying's own form of loss aversion motivated him to engage in insider trading? Why or why not?
5. Do you think a company that holds personal identifying information of consumers is ethically obligated to inform consumers of every data breach? Why or why not? Are there instances when a company should withhold information from consumers? Explain your reasoning.
6. Can you think of other companies that faced a data breach in which users' personal information was compromised? How did the company respond? Do you think the company demonstrated loss aversion? Why or why not?
7. Can you think of other situations you have read about where companies made innocent mistakes, but then intentionally covered them up? How does the potential for huge civil damage liability affect people's inclination to admit mistakes?
8. Dennis Gentilin suggests that loss aversion is a very significant driver of wrongdoing by leaders because, of course, they have more to lose: "There is a driver of behavior within organisations that goes beyond money and power. People within organisations, especially the most senior and powerful, have worked for years to attain a status or title that they become highly attached to, is central to their identity, and defines who they are. When their position is threatened, be it due to poor performance, feelings of incompetence, changes in organizational structure or the risk of having previous maleficence uncovered, the natural response is to go to extreme lengths to defend and protect this position. What is driving this defensive response is the fear associated with the loss of their status and title, and the associated financial rewards and lifestyle the position affords. By extension, what is at stake is their very sense of self and identity." Does this ring true to you? Discuss.
9. Do you find it difficult to admit your own mistakes? Do you think it is difficult for most people to admit their mistakes? Explain.
10. Equifax's case demonstrates the pitfalls of a number of biases and behaviors including moral myopia, conformity bias, and groupthink. Can you identify these and other behavioral ethics concepts at work in this case study? Explain and discuss their significance.

Bibliography:

A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

<https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/>

As Equifax Amassed Ever More Data, Safety Was a Sales Pitch

<https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html>

Massive Equifax Data Breach Could Affect Half of the U.S. Population

<https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686>

Equifax's Massive Hacking Scandal Could Cost \$70 Billion

<https://www.vanityfair.com/news/2017/09/equifax-hack-lawsuit>

Equifax website hack exposes data for ~143 million US consumers

<https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/>

Equifax Can't Protect Data, But It Can Keep a Secret

<https://www.bloomberg.com/gadfly/articles/2017-10-03/equifax-can-t-protect-data-but-it-can-keep-a-secret>

Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed

<https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed>

Equifax Was Warned

https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning

Failure to patch two-month-old bug led to massive Equifax breach

<https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/>

Three Equifax Managers Sold Stock Before Cyber Hack Revealed

<https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack>

Ex-Equifax Executive Charged With Insider Trading Tied to '17 Breach

<https://www.nytimes.com/2018/03/14/business/equifax-executive-insider-trading.html>

Senior ex-Equifax executive charged with insider trading

<https://arstechnica.com/information-technology/2018/03/senior-equifax-executive-charged-with-insider-trading/>

Consumers have filed thousands of complaints about the Equifax data breach. The government still hasn't acted.

<https://www.vox.com/policy-and-politics/2018/4/30/17277172/equifax-data-breach-cfpb-elizabeth-warren-mick-mulvaney>

The Origins of Ethical Failures: Lessons for Leaders

<https://www.worldcat.org/title/origins-of-ethical-failures-lessons-for-leaders/oclc/971052714>