LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS5052NI PROFESSIONAL ISSUES ETHICS AND COMPUTER LAWS

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2020-21 Spring

Student Name: MD OSHAMA
London met ID: 19031129
College ID: NP01CP4A190177

Assignment Due Date:14th May 2021
Assignment Submission Date: 14th May 2021

Title: Research on Equifax

Word Count:4955

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Table of Content

Contents

Introduction

Equifax is a global data, analytics, and technology company. We believe knowledge drives progress. We blend unique data, analytics, and technology with a passion for serving customers globally, to create insights that power decisions to move people forward. Headquartered in Atlanta, Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX. Equifax employs approximately 11,000 employees worldwide.

In March 2017, personally identifying data of hundreds of millions of people was stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States. Equifax was criticized for everything ranging from their lax security posture to their bumbling response to the breach, and top executives were accused of corruption in the aftermath. And the question of who was behind the breach has serious implications for the global political landscape.

The crisis began in March of 2017. In that month, a vulnerability, dubbed CVE-2017-5638, was discovered in Apache Struts, an open-source development framework for creating enterprise Java applications that Equifax, along with thousands of other websites, uses. If attackers sent HTTP requests with malicious code tucked into the content-type header, Struts could be tricked into

executing that code, and potentially opening up the system Struts was running on to further intrusion. On March 7, the Apache Software Foundation released a patch for the vulnerabilities; on March 9, Equifax administrators were told to apply the patch to any affected systems, but the employee who should have done so didn't. Equifax's IT department ran a series of scans that were supposed to identify unpatched systems on March 15; there were in fact multiple vulnerable systems, including the aforementioned web portal, but the scans seemed to have not worked, and none of the vulnerable systems were flagged or patched.

While it isn't clear why the patching process broke down at this point, it's worth noting what was happening at Equifax that same month, according to Bloomberg Businessweek: Unnerved by a series of incidents in which criminals had used Social Security numbers stolen from elsewhere to log into Equifax sites, the credit agency had hired the security consulting firm Mandiant to assess their systems. Mandiant warned Equifax about multiple unpatched and misconfigured systems, and the relationship devolved into in acrimony within a few weeks.

Like plane crashes, major infosec disasters are typically the result of multiple failures. The Equifax breach investigation highlighted a number of security lapses that allowed attackers to enter supposedly secure systems and exfiltrate terabytes of data.

The company was initially hacked via a consumer complaint web portal, with the attackers using a widely known vulnerability that should have been patched but, due to failures in Equifax's internal processes, wasn't.

The attackers were able to move from the web portal to other servers because the systems weren't adequately segmented from one another, and they were able to find usernames and passwords stored in plain text that then allowed them to access still further systems.

The attackers pulled data out of the network in encrypted form undetected for months because Equifax had crucially failed to renew an encryption certificate on one of their internal security tools.

Equifax did not publicize the breach until more than a month after they discovered it had happened; stock sales by top executives around this time gave rise to accusations of insider trading.

Legal Issue

Federal agencies, state officials and members of Congress are now probing Equifax (EFX) over its data security practices, customer service response and the possibility of insider trading from executives. *(BUSINESS, 2017)*

The breach may have compromised personal information from as many as 143 million Americans. This included some of our most sensitive information: social security numbers, addresses, driver's license numbers.
(BUSINESS, 2017)

A rush of lawsuits has also been filed against Equifax on behalf of consumers and shareholders. And that's just in the US.

Equifax said Tuesday that as many as 100,000 Canadians may have been impacted by the breach. Last week, the company said up to 400,000 people in the U.K. may had personal information compromised too.

Federal Trade Commission probe:

In an unusual move, the FTC said last week that it has opened a probe into the Equifax debacle. The agency did not specify which aspects of the breach it's investigating.

Massachusetts and other states:

Maura Healey, the attorney general of Massachusetts, filed the first state lawsuit against Equifax on Tuesday. Healey alleges Equifax "knew about the vulnerabilities in its system for months, but utterly failed" to keep customers safe. *(BUSINESS, 2017)*

Congressional hearings:

Equifax has come under fire from legislators of both parties. The House Financial Services Committee and the House Energy and Commerce Committee have each called for hearings on what went wrong leading up to the breach.

Senate pressure over stock sales:

Separately, a bipartisan group of dozens of senators sent a letter urging the FTC, Department of

Justice and the Securities and Exchange Commission to investigate Equifax over its executives' stock sales.

Three Equifax executives sold shares of their company worth nearly $2 million shortly after the breach was discovered. The sales came before the breach was announced to the public. *(BUSINESS, 2017)*

Dozens of private lawsuits:

Given the scale of the breach, it should come as little surprise that Equifax is inundated with private litigation. Dozens of class action lawsuits have already been filed against Equifax on behalf of consumers and shareholders. *(BUSINESS, 2017)*

The Equifax breach has captured the attention of local, state, and federal governments in the U.S. as well as UK and Canadian regulators.

Local Governments

The cities of San Francisco and Chicago have sued Equifax. San Francisco's complaint alleges violations of California's unlawful, unfair or fraudulent business practices law when it (1) failed to implement and maintain reasonable security practices; (2) failed to provide timely notice of the breach; and (3) failed to provide clear and complete information. It seeks restitution for California consumers who purchased credit monitoring services from Equifax prior to the announcement of the breach, up to $2,500 for each violation of the law, and a court order requiring Equifax to implement and maintain appropriate security procedures. Chicago's complaint alleges violations of the Illinois Personal Information Privacy Act, the Illinois Consumer Fraud and Deceptive Business Practices Act and the Chicago Consumer Fraud ordinance for (1) exposing personal information; (2) failing to provide timely notice of the breach; and (3) misleading consumers by representing its credit monitoring service as complimentary when it included a mandatory arbitration clause that barred users of the service from bringing future legal action against Equifax. *(epic.org, 2021)*

State Governments

State attorneys general have been active in responding to the breach. Maura Healey, the Attorney General of Massachusetts, brought an enforcement action against Equifax. The complaint alleges violations of Massachusetts consumer protection and data privacy laws. New York's Attorney

General Eric Schneiderman introduced the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). The bill would (1) require any business that holds sensitive data of New Yorkers to adopt reasonable administrative, technical, and physical safeguards; (2) expand the types of data that trigger reporting requirements, to include username-and-password combinations, biometric data, and HIPAA-covered health data; and (3) provide safe harbor protection for companies that obtain independent certification that their data security measures meet the highest standards. The attorneys general of Connecticut, Illinois, Pennsylvania, and the District of Columbia sent a joint letter to Equifax notifying the company of their intent to investigate the breach. The letter was signed by the attorneys general of dozens of other states. *(epic.org, 2021)*

Federal Government

The federal government is also conducting investigations. In a rare move by the Federal Trade Commission, Peter Kaplan, the agency's acting director of public affairs, confirmed that the agency is investigating the Equifax breach. The Consumer Financial Protection Bureau is also investigating the company, though recent reports indicate that the agency may be pulling back from its probe. The SEC and U.S. attorney’s office in Atlanta (where Equifax is headquartered) are investigating Equifax for insider trading related to the sale of stock by executives before the breach was announced to the public. *(epic.org, 2021)*

Social Issues

Equifax specifically traffics in personal data, and so the information that was compromised and spirited away by the attackers was quite in-depth and covered a huge number of people. It potentially affected 143 million people — more than 40 percent of the population of the United States — whose names, addresses, dates of birth, Social Security numbers, and drivers' licenses numbers were exposed. A small subset of the records — on the order of about 200,000 — also included credit card numbers; this group probably consisted of people who had paid Equifax directly in order to order to see their own credit report.

This last factor is somewhat ironic, as the people concerned enough about their credit score to pay Equifax to look at it also had the most personal data stolen, which could lead to fraud that would then damage their credit score. But a funny thing happened as the nation braced itself for the wave of identity theft and fraud that seemed inevitable after this breach: it never happened. And that has everything to do with the identity of the attackers.

Equifax Inc. (EFX) announced on Sept. 7, 2017 that 143 million of its customers were affected by a hack that occurred between mid-May and July. That figure was bumped to 145.5 million over the following weeks, then to 147.9 million on Mar. 1, 2018, when the company said it had identified 2.4 million additional victims. *(Investopedia.com, 2021)*

After market close the same day, the company reported fourth-quarter and full-year financial results. The company's fourth-quarter revenues rose 5% year-over-year to $838.5 million. Net income in the quarter rose 40% year-over-year to $172.3 million. Full-year revenues and profits also rose compared to 2016: revenues were up 7% to $3.4 billion, while net income increased 20% to $587.3 million. The company said the hack had cost it $26.5 million in the fourth quarter and $114.0 million in the full year, net of insurance payouts. The stock, which closed down 1.3% in line with the S&P 500, is up 0.6% in after-hours trading at the time of writing.

As many as 209,000 customers' credit card numbers were exposed, according to Equifax, and dispute documents related to 182,000 U.S. consumers – which include personal information – were compromised. British consumers were also have been affected by the breach; it is possible that some

Canadians were compromised. According to The Wall Street Journal, citing an unnamed source, 10.9 million Americans' drivers license data was stolen in the breach.

The company had known about the attack since July 29, but waited over a month to alert the public. On Sept. 20 it was reported that Mandiant, the FireEye Inc. (FEYE) subsidiary contracted by Equifax, estimates the breach to date back to at least March 10.

There is little information regarding the source of the attack, which is being investigated by the FBI, but according to Bloomberg, similarities to earlier attacks on the Office of Personnel Management and Anthem Inc. suggest the attacker could be state-sponsored, perhaps Chinese. That Equifax customers' information has not shown up on the black market also suggests the hackers were not simply criminals. Bloomberg also reports that the attackers targeted specific individuals, perhaps because of their wealth or intelligence value.

Given that the adult population of the U.S. is around 250 million, chances are good that you were affected by the breach. It is also possible that you have already been a victim of fraud, since the attack began nearly six months ago.

Atlanta-based Equifax, one of the big three consumer credit reporting agencies – the other two are Experian PLC (London: EXPN) and TransUnion (TRU) – collects data including Social Security numbers, credit card numbers, driver’s license numbers, rent and utility payment information, and demographic data. Because Equifax's model is primarily business-to-business, many of its customers are unaware that their data is stored by the firm. Aside from avoiding the financial and credit system altogether, there is no straightforward way to opt out of having personal data stored by Equifax. *(Investopedia.com, 2021)*

Equifax's then-chairman and CEO, Richard Smith, said after the hack that it was "clearly a disappointing incident for our company, and one that strikes at the heart of who we are and what we do." He stepped down on Sept. 26 and will not receive a bonus for 2017. His departure followed those of chief security officer Susan Mauldin and chief information officer David Webb on Sept. 14.

A few days after the company uncovered the hack internally – and before the breach was revealed to the public – Equifax's chief financial officer John Gamble, its president of workforce solutions Rodolfo Ploder, and its president of U.S. information solutions Joseph Loughran sold their Equifax shares. Equifax said in a statement that the executives did not know about the breach when they sold their stock. Gamble, Ploder and Loughran collectively earned nearly $1.8 million from the sales.

As of Feb. 28, Equifax's stock has fallen 20.1% from its close on Sept. 7 (before the hack was announced) to $113.00. After several delays, Equifax says it will report fourth-quarter earnings after close on Mar. 1.

Reuters reported on Sept. 11 that more than 30 lawsuits – many of them seeking class action – have been filed against Equifax in U.S. courts. Several allege violations of securities law; others accuse TrustedID of pitching costly services to customers who were affected by the data breach. Five Utah residents have sued the company in U.S. District Court for failure to protect customers' sensitive data. The suit seeks monetary damages of $5 billion and the imposition of stricter industry standards.

A few affected customers are taking a less traditional route in seeking recourse from Equifax. The DoNotPay chatbot provides assistance in filing a complaint in state small claims courts, where maximum penalties range from $2,500 to $25,000. The bot can only generate paperwork for a lawsuit, not actually file it or appear in court, according to the Verge. *(Investopedia.com, 2021)*

Ethical Issues

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. *(Unwrapped, 2021)*

Equifax, like its two rivals, is the gateway to consumers' access to financial credit. Equifax's customers also include the users of this data to make credit decisions. If you had to boil down the two most core ethical principles that were required of Equifax given these unique roles, it should be integrity and security.

Ironically, Equifax updated and reissued its corporate code of ethics in July, about the same time it discovered the breach. Equifax's code touts the importance of honesty and fair dealing in maintaining appropriate business relations, protecting the privacy and confidential information of others, advising employees to watch out for company property that is not secured, and prohibition of insider trading. Former Chairman and CEO, Richard F. Smith has an introductory message to the code discussing his commitment to the code and compliance.

Equifax used an open-source software tool known as Apache Struts that supported Equifax's online dispute portal web application. The company believes that the hackers gained access to its data through a vulnerability in Apache Struts. This vulnerability was known to Equifax since March 2017. The hackers gained access to Equifax's data from May 13 through July 30th, when Equifax took down this web portal.

Why didn't Equifax take down the web portal as soon as it knew the software was vulnerable, and not brought the portal back up until the security flaw was patched?

Companies lacking in internal controls tend to be more exposed to ethical failings than companies with strong internal controls. We normally think of accounting processes when we discuss a company's internal controls, but its internal controls over its computer systems are equally important, especially for a company whose product is digitally maintained.

Equifax has not said why they waited until September 7th before announcing the cyber incident. Could it be that the hacking was too embarrassing for a proud company to announce, or was there another reason?

This delay deprived its customers the opportunity to take early actions to mitigate the potential damage from the exposure of their personal data. Credit freezing and monitoring could have started months ago.

The creditors and financial institutions that rely on Equifax were considering credit applications and approving loans for this period. They were totally unaware that the applications they were processing could be fraudulent and contain personal information stolen from Equifax. These companies were unable to consider whether they required other forms of identification and information to verify that they were not processing credit applications for fraudsters.

Ethical conduct of companies and executives is a hot-button topic in corporate America precisely because ethical failures are commonplace. Equifax is one example of many. An ethics policy or code is only as good as the leadership implementing it. People are fallible and do things that others will simply say, "What were they thinking?", when unethical conduct is exposed, as it almost always is.

Equifax's problems could have been prevented if certain executives had followed the company's code of ethics, their individual personal values and common sense. But, this is a prime example how a lapse in ethics can have a significant adverse impact on 143 million consumers and countless institutions that rely of quality credit information to conduct their business. *(BEA, 2021)*

Professional issues

In the wake of the Equifax computer breach—in which key personal information of 145 million Americans was stolen—it may be correct to assume that anyone with a credit history is affected. In the words of noted cybersecurity expert Brian Krebs, “Assume you’re compromised, and take steps accordingly” (“Fear Not: You, Too, Are a Cybercrime Victim,” KrebsonSecurity.com, Oct. 17, 2017, http://bit.ly/2A67XLX). For professionals, there are broader cybersecurity concerns, as CPA firms of all sizes have recently been hacked, from local firms whose stolen client Social Security numbers were used to divert clients’ IRS tax refunds to firms that have been subject to ransomware extortion.

Over the past decade, over 3 billion people’s personal information has been hacked from email providers like Yahoo or retailers like Target. The Equifax breach, however, is the first in which the “big four” personal security identifiers—name, address, birth date and Social Security number—were stolen from so many at once. These are the security authentication foundations for many commercial and other purposes (Robert Lemos, “Identity Verification Becomes Trickier in Wake of Equifax Breach,” eWeek, Sept. 11, 2017, http://bit.ly/2yMVLOu).

Possession of these identifiers may increase two forms of identity theft: new account fraud and account takeover. In new account fraud, a criminal uses the identifiers and possibly other information to open new credit accounts in a person’s name; the target does not find out until his credit rating is wrecked after the bills go unpaid. The aggravation, costs, and time spent on the resulting credit repair can be significant. In account takeover, the criminal uses the four identifiers to impersonate someone for various purposes, including creating fraudulent transactions. To CPA firms, one of the more familiar frauds of this type is the filing of phony income tax returns to steal tax refunds. In some cases, local CPA firm computers have been breached, enabling thieves to successfully perpetrate this type of fraud.

Recently, account takeover has been used to steal cell phone numbers, which can compromise

multifactor authentication (MFA), an important cybersecurity best practice (Nathaniel Popper, "Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency," New York Times, Aug. 21, 2017, http://nyti.ms/2jws7dq). MFA requires providing authenticating information in a manner different than the initial authentication; for example, some websites will, after the user has inputted her password, send a second verification code via text message that must also be inputted to log in. Another MFA method requires that the initiator make a call from a predetermined phone number; unfortunately, such a phone number can be imitated, and the security of the MFA rendered ineffective.

Weak MFA approaches could lull CPAs into a false sense of security. Many accounting software programs rely on two-factor authentication for sign-in or to reset forgotten passwords, and an increasing number of these programs enable the electronic transfer of funds from bank and investment accounts. With this type of account takeover on the rise, it may be wise to revisit the use of cellphone text messages for MFA, as well as explore more secure approaches.

In previous major breaches, the public attitude has generally been to accept the risk as the price of convenience. The Equifax breach, however, has taken public frustration over weak cyber-security to unprecedented levels (Ron Lieber, "Why the Equifax Breach Stings So Bad," New York Times, Sept. 22, 2017, http://nyti.ms/2jvZvkT). The breach is beginning to instill general fear that the cybersecurity underpinning electronic commerce cannot be trusted.

Since the beginning of e-commerce, there has been a tug of war between the desire for fast and frictionless transactions and the need for extra, inconvenient security steps. The Equifax breach may swing the pendulum towards security. The sections below address the protective steps that should be taken by CPA firms and their clients to create an appropriate level of cybersecurity. *(CPA_Journal, 2021)*

CRAs have become gatekeepers for essential functions, like finding work, housing, and managing one's money. Consumers need credit to navigate the current economic system. While we might be able to choose not to shop at Amazon, for example, electing not to establish a credit history amounts to opting out of regular economic activity. Consumers therefore lack agency in their relationship with CRAs.

Information held by CRAs, including PII, is especially sensitive. Other businesses wouldn't have access to this type of data. Loss of PII can result in identity theft with devastating effects, including financial instability, and lack of access to housing and employment, for consumers. Further, this loss of PII means credit information supplied to lenders is no longer reliable or valuable.

Loss of information through data breaches not only threatens the validity of the credit reporting industry's function but also threatens the United States' national security and economic infrastructure. The current banking and taxation system utilizes social security numbers as PII. According to security investigators, the Equifax data breach was most likely the work of the Chinese government as part of a scheme to collect pools of consumers' data. It's not a stretch to imagine that a hostile international actor could use consumer data to significantly disrupt these systems. *(sevenPillarsinstitute.org, 2021)*

Conclusion

"Most people think that cybersecurity standards are over complex and demanding. However, the truth is they need to be as comprehensive as they are in terms of the range of security controls needed in order to get anywhere near a state of what could be called secure IT operations," notes Mark Kedgley, CTO at New Net Technologies (NNT), a Naples, Florida-based provider of IT security and compliance software. "Automation is the only way to deal with the scale of today's Enterprise IT infrastructure but too many organizations are still short of where they need to be in terms of the foundational controls such as vulnerability management, configuration hardening and change control."

According to Kedgley, the autopsy reports of the Equifax breach list a number of fatal failures – corners were cut on key security controls which were then compounded by human error and gaps in critical processes to address vulnerabilities. "A lack of change control and breach detection visibility then left systems compromised for months. Key lesson is that it isn't enough to just have some security controls and products in place, effective cybersecurity requires a pervasive adoption of security best practices at all levels throughout an organization. Frankly, too many chances were missed to prevent the breach, detect the indicators of compromise and do the right thing when the real picture was understood. However, it can serve as a great example of why cybersecurity really matters."

Tom Pendergast, Chief Learning Officer at MediaPro, a Seattle, Washington-based provider of cybersecurity and privacy education, says that the core actions that could have prevented the Equifax breach—effective patching and network segmentation—were well known to all before the breach. "So the question is: if we know how to protect ourselves, why don't we? You'll hear excuses like we don't have the budget, we don't have the time, we don't have enough personnel. But it all comes down to complacency: we either don't think it will happen to us, we're not able to convince others that the risk is real, or it just feels like an insurmountable challenge," adds Pendergast. "Some lessons learned since Equifax include patch, segment your networks, train on appropriate incident reporting (to flag issues as soon as possible). Hopefully, business leaders will have a better recognition of what's required to secure the organization against cybercrime. Infosec leaders need the support of the business to put protections in place—and incidents like Equifax help make the case for budget, staff, and training to secure the organization."

Charles Ragland, security engineer at Digital Shadows, a San Francisco-based provider of digital risk protection solutions, notes that, "Mature security program results don't always manifest themselves in prominent ways, which unfortunately leads many organizations to place security on the back burner. When treating security as a box-checking exercise, and not a workplace culture, organizations are often surprised when an incident happens."

"Creating realistic risk management frameworks for vulnerability assessment results is one of the top ways to maintain your security posture and reduce your attack surface," adds Ragland. "Evaluating the difference between vulnerable and exploitable systems and making decisions based on business needs and risk tolerance is crucial for organizations to prevent an Equifax-style attack." *(SECURITY, 2021)*

At any rate, once the breach was publicized, Equifax's immediate response did not win many plaudits. Among their stumbles was setting up a separate dedicated domain, equifaxsecurity2017.com, to host the site with information and resources for those potentially affected. These sorts of lookalike domains are often used by phishing scams, so asking customers to trust this one was a monumental failure in infosec procedure. Worse, on multiple occasions official Equifax social media accounts erroneously directed people to securityequifax2017.com instead;

fortunately, the person who had snapped up that URL used it for good, directing the 200,000 (!) visitors it received to the correct site.

Meanwhile, the real equifaxsecurity2017.com breach site was judged insecure by numerous observers, and may have just been telling everyone that they were affected by the breach whether they really were or not. Language on the site (later retracted by Equifax) implied that just by checking to see if you were affected meant that you were giving up your right to sue over it. And in the end, if you were affected, you were directed to enroll in an Equifax ID protection service — for free *(CSO, 2021)*

Ethical conduct of companies and executives is a hot-button topic in corporate America precisely because ethical failures are commonplace. Equifax is one example of many. An ethics policy or code is only as good as the leadership implementing it. People are fallible and do things that others will simply say, “What were they thinking?”, when unethical conduct is exposed, as it almost always is.

Equifax’s problems could have been prevented if certain executives had followed the company’s code of ethics, their individual personal values and common sense. But, this is a prime example how a lapse in ethics can have a significant adverse impact on 143 million consumers and countless institutions that rely of quality credit information to conduct their business. *(BEA, 2021)*

Thank You

Bibliography

BEA. (2021). *Business Ethics Advisors*. Retrieved from https://johnkevinfoster.com/equifax-data-breach/

BUSINESS, C. (2017, 09 19). *CNN BUSINESS*. Retrieved from https://money.cnn.com/2017/09/19/technology/equifax-legal-issues/index.html

CPA_Journal. (2021). Retrieved from https://www.cpajournal.com/2017/12/15/equifax-data-breach/

CSO. (2021). Retrieved from https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

epic.org. (2021). *epic.org*. Retrieved from epic.org: https://epic.org/privacy/data-breach/equifax/#:~:text=Summary,million%20Americans%20had%20been%20compromised.&text=The%20credit%20card%20numbers%20of%20approximately%20209%2C000%20consumers%20were%20also%20breached.

Investopedia.com. (2021). *Investopedia*. Retrieved from https://www.investopedia.com/news/was-i-

hacked-find-out-if-equifax-breach-affects-you/
SECURITY. (2021). Retrieved from https://www.securitymagazine.com/articles/93282-lessons-learned-from-the-equifax-data-breach
sevenPillarsinstitute.org. (2021). Retrieved from https://sevenpillarsinstitute.org/case-study-equifax-data-breach/
Unwrapped, E. (2021). Retrieved from https://ethicsunwrapped.utexas.edu/video/equifaxs-breach-of-trust