LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

**Module Code & Module Title**

**CC4004NI Cyber Security Fundamentals**

**Assessment Weightage & Type**

**50% Individual Coursework**

**Year**

**AY 2023 - 2024**

**Student Name: pradip joshi**

**London Met ID: 23047485**

**College ID: np01nt4a230162**

**Assignment Due Date: Sunday, May 5, 2024**

**Assignment Submission Date: Sunday, May 5, 2024**

**Word Count: 3273**

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

PRADIP JOSHI

## Contents

## Table of figures

## Abstract

One of the biggest credit reporting company Equifax was the victim of the apt attack where the names, addresses, birth dates, Social Security numbers, and driver's permit numbers, PII(personally identifying information) of a lot of people was affected in 2017. The main purpose of this report was to study about that attack and try to evaluate the different aspects of the attack by different ways. This report contains the details about the attack exposing how the attack occurred, what or who was responsible for this attack and most importantly how were the customers and the company itself was affected from this attack.

This report also focuses on exposing the mistakes made by the company itself that led to the attack of that level on the company of that level. This report also contains information about how the company failed to find and patch the vulnerability even after knowing about the it. What type of fines are imposed on the company that suffers from the cyber-attacks and what lessons other companies should get from this attack is also discussed in this report. This report also gives the insights on what the CISO of that company should have done before and after the attack.

It is suggested to have a basic level of understanding on cyber security to get the complete understanding on what the report tries to tell.

# 1. Introduction

## 1.1. Introduction

Every year, there is an increasing number in the worldwide cyber threat with the increasing numbers of incidents of data breach simultaneously. In just first nine months of 2019**, 7.9 billion** records were compromised, according to report released by Risk Based Security. As the worldwide threat presented by cybercrime continues to grow. Businesses are also making greater expenditures in cyber security solutions to protect themselves from cyberattacks. According to study and advisory firm Gartner, global spending on security measures will go above **$188.3 billion** by 2026.  Because they hold financial and medical data, attackers typically target government agencies, shops, and organizations that use networks to deliver their services. (kaspersky, 2024).

**8,214,886,660** records were hacked as a result of **2,814** security incidents that were recorded in 2023 alone (Ford, 2024). Surprisingly**, 5,360** cybersecurity incidents had been made public as of March 5th, this year, compromising about **30,272,408,782** records. (Ford, 2024).

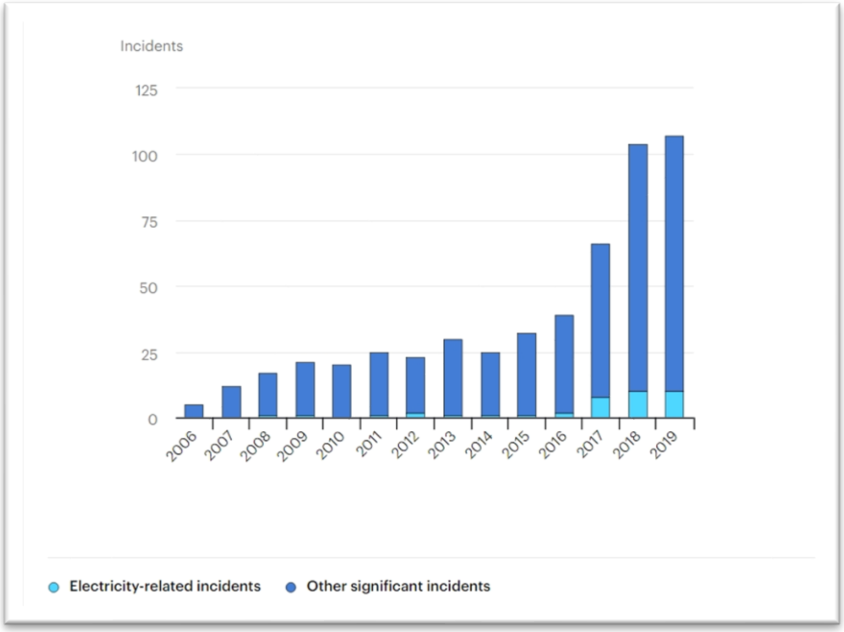

*Figure 1: Significant cyber incidents worldwide, 2006-2019 (International Energy Agency (IEA), 2020)*

The given graph shows the significant cyber incidents worldwide, 2016-2019.

The credit report establishment Equifax revealed that it had gone through an information breach in 2017. Equifax said that among the data that was hacked were client names, driver's permit numbers, address, social security numbers, and birth dates. Besides, around **209,000** credit card numbers and **182,000** US consumer’s dispute documents that contained PII were also compromised. (john, 2017).

Therefore, we will be exploring about this case in this report.

## 1.2. Technical Terminologies used in this report

### 1.2.1. cyber attack

Cyberattacks are attempts to obtain unauthorized access to a computer system or network with the intention to steal, alter, or destroy data, among other criminal activities (Microsoft, 2022).

### 1.2.2 APT

A type of attack where the attacker tries to stay hidden for a period of time after entering the targeted network is called APT attack. (CISCO, 2024)

### 1.2.3. Vulnerability

Vulnerabilities are the system's weakness that gives threat actors the chance to compromise the company's assets (geeksforgeeks, 2020).

### 1.2.4 . Encryption

The technique of converting data such that only those with the key to reverse it can use it. (Google Cloud, 2020).

### 1.2.5. Database

A database is an organized collection of structured data that is kept in a computer system (Oracle, 2020).

### 1.2.6. Policy

A policy is a set of guidelines that specify how data from an establishment should be stored, managed, and shared in order to reduce the danger of cyberattacks (hackerone, 2024).

### 1.2.7. CISO(chief information security officer)

An administrative officer of the senior level who manage information, cyber, and technological security for the business (CISCO, 2024).

### 1.3 About Equifax

In 1899, Banking and credit reporting company Equifax was founded. It’s headquarter is located in Atlanta, Georgia. It is one of the three major credit reporting agencies in the United States, along with Transunion and Experian. Another additional name for them is "**the Big three**" (Miyashiro, 2021). It is a top global data, analytics, and technology corporation that uses cloud computing to grow the world economy. It analyzes the various data from the consumers and commercial business databases. The data includes credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data. (equifax, 2023).

*Figure 2: Equifax Inc. (freebie supply, 2024)*

## 1.4. Aims and objectives

This report aims to give a data breach information’s of the 2017 Equifax Inc. data breach incident. Its objectives are as follows:

1. To comprehensively study about what, when and how did it happened.
2. To investigate how the organization and its clients were affected.
3. To study about the fines and penalties that regulatory bodies might apply in response to security breaches.
4. To know about proactive methods to stop the incident from happening and look at measures that should be performed after the incident to stop them from occurring again.
5. To identify the lessons to be learned from the Equifax data breach incident.

# 2. SECTION 1: Research into the theft of personal data

## 2.1. How were the costumers affected?

In September 2017, the credit-reporting company Equifax reported that attackers had obtained access to different website applications software. It is estimated that the hackers accessed the private data of **143 million** clients. Individuals' names, addresses, birth dates, Social Security numbers, and driver's permit numbers were among the data affected. Also, credit card details of **209,000** US customers were taken, and debate records counting the private data of **182,000** clients were compromised too (Bracy, 2017).

In 2018, a survey was conducted. The majority of those questioned knew a good deal about the incident. A lot of Americans were worried about their data being compromised. **57.2** percent of the people who were asked said they investigated whether their data was hacked. Unfortunately, **35.5%** of individuals discovered that their information was compromised. The decision of whether to store their data in the Equifax system was not left up to the consumers was the challenging aspect for them. **54.2** percent of answers to the 2017 study said they wanted Equifax to shut down as a credit reporting agency; however, within a year of the incident, this percentage dropped to **46.2** percent (Brown, 2018).

## 2.2. How did the breach occur?

The US Computer Emergency Readiness Team released a vulnerability report on **March 8, 2017**, and according to Equifax, unknown people explored the company's systems after two days to see if there was a presence of the same vulnerability. Attackers could gain control of compromised systems by exploiting that vulnerability within the Apache Struts Web Framework.

As a result of their search, those individuals found a server housing the company's online dispute portal was using a version of the program that was vulnerable.

A software that was specially designed to exploit the vulnerability in Apache struts to gain access to the Equifax portal was used by the attackers. By doing so they made sure that they could run commands.

Equifax reports that attackers gained access to the online dispute portal on **May 13,2017.** In a second incident that happened after the original illegal access. Different types of strategies were used by them to hide their activity. The attackers used the encrypted communication channels that were linked to the online dispute site to send instructions and queries to other systems and call the personally identifiable information that was saved on those systems. By using encryption of communication channel, the attackers were able to stay hidden on the Equifax network and carry out more illegal activities without being caught by Equifax's scanning software. The encryption also allowed them to mix in their criminal activity with normal network activity.

After the attackers were able to give commands at the system level on the compromised online dispute portal, they queried additional databases in the attempt to find sensitive information. A data repository with PII and unencrypted usernames and passwords of multiple other Equifax databases was found as a result of this search. The attackers were able to use those credentials to get access to **48 more unconnected** databases that were not linked to the online dispute system. At first, they had access to only **3 databases**. All these information was given by chief information security officer (CISO) .

The attackers then executed a number of queries in an attempt to collect PII from the databases they had identified, according to Equifax personnel who had reviewed system log files that documented the attacker’s operations. The attackers executed about 9,000 requests in all, some of which were successful in returning information that contained personally identifiable information.

After their successful extraction of personally identifiable information from Equifax databases, the attackers gradually deleted the information while hiding their interactions as regular network traffic using standard encrypted web protocols. Before it was detected, the attack continued for around **76 days**. (Government Accountability Office (GAO), 2024). All the given steps are presented in the image given below.

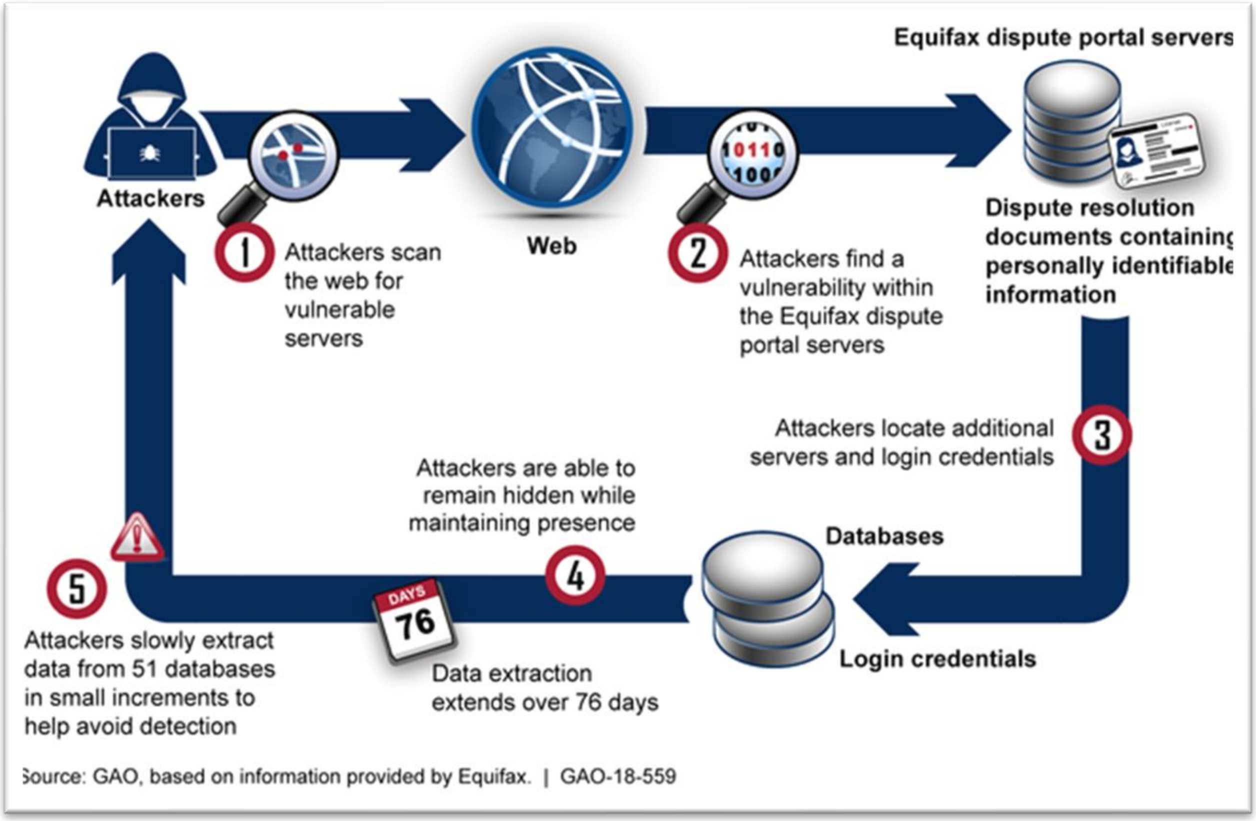
Equifax dispute portal servers
Attackers
Web
1 Attackers scan the web for vulnerable servers
2 Attackers find a vulnerability within the Equifax dispute portal servers
Dispute resolution documents containing personally identifiable information
3 Attackers locate additional servers and login credentials
Databases
Login credentials
4 Attackers are able to remain hidden while maintaining presence
DAYS 76
Data extraction extends over 76 days
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection
Source: GAO, based on information provided by Equifax. | GAO-18-559

*Figure 3: Analysis of How Attackers Exploited Vulnerabilities (Government Accountability Office (GAO), 2024)*

## 2.3. What were the mistakes made by Equifax?

The vulnerability, recognized as **CVE-2017-5638**, which was built into Apache Struts, allowed the attackers to carry out the attack. Equifax states that the online dispute portal web application is supported by the open-source application system Apache Struts (equifax, 2017). Equifax claimed to have been aware of the vulnerability for two months before the attackers gained access (Jackie Wattles, 2017).

The given points try to properly describe errors that lead to the data breach:

1. Failure to patch the vulnerability that was present in Apache Struts (CVE-2017-5638) on time even after being aware of the vulnerability about two months before the attackers gained access to the system (Jackie Wattles, 2017).
2. poor response time: Equifax took approximately five months to implement the necessary patch, far exceeding the 48-hour limit defined by their security protocol.
3. Lack of an IT Asset Inventory system: Due to the absence of this system Equifax wasn't aware of the locations of the vulnerable application i.e. (Apache struts) in the system Which made it difficult for Equifax to efficiently find and patch vulnerability on time.
4. Ineffective detection measures: Equifax did many network scans but couldn't find any cases of defective software.
5. Failure to follow up: The management team tried to find the vulnerability in the software but after failure of several effort, they didn't take any other actions to find and remove the vulnerability (Miyashiro, 2021).
6. Lack of segmentation: According to Equifax officials, the attackers were able to access databases other than those connected to the online dispute center. This was possible because individual databases were not segmented from one another. The lack of segmentation gave the attackers access to more PII-containing databases and allowing them to successfully remove a lot of PII without raising an alarm (Government Accountability Office (GAO), 2024).

It takes time for large organizations with numerous machines to fix their software. To guarantee security, the vulnerability must first be located, the patch must be created, and testing is required. All of these steps require time.

However, Jon Hendren director of strategy at security company UpGuard said "**There's really no excuse whether it's a difficult patch or not, for an organization of that size with that kind of magnitude of data**,". He added **"When you're a big organization like that, it's a systemic failure of process and the blame goes straight to the top."** (Jackie Wattles, 2017)

Considering all the above information, it appears that a major contributing factor to the Equifax data breach was a failure to adopt a proactive approach and failure to exercise due care.

## 3. SECTION 2: Personal data loss in a cyber-attack

Rather than panicking in an unfortunate event of the organization being hacked or the data being breached, the organization should focus to take proper action which can help to reduce the chances of the problem being more vital (Marsh Commercial, 2022).

Once the company is aware that it has been attacked, it can carry out the following actions.

Firstly, company has to find any necessary proof, protect it, make sure nothing is lost or destroyed, turn on the incident response plan, disconnect the network from the Internet, make a list of everyone who was in the company before, during, and after the incident, and establish a point of contact with whom law enforcement officials can get in touch to discuss the incident and obtain information.

Secondly, the report number provided by the law enforcement should be documented by the company. It should also be ready for the possibility that law enforcement will require access to the equipment in order to investigate the technical details of the cyber event. It is important to work with police to collect evidence while causing a small amount of interruption to ongoing operations and recovery plans. The business should also provide letters, employee statements, logs, and any other appropriate paperwork as additional evidence. It should also create a list of significant contacts in its organization for law enforcement.

At last, the company should inform its partners, customers, employees, and other stakeholders about the event. It should review its cyber security policies and ensure that the employees get training. Antivirus and anti-malware software for devices and networks should be purchased and defensive measures like virtual private networks, firewalls, and encryption should be implemented in place to improve data security and get ready to testify in court if needed (Royal Canadian Mounted Police, 2021).

### 3.1. Fine imposed on the Equifax by the government bodies

The Information Commissioner's Office, which was set up to guard information rights in the UK (BBC, 2018), fined Equifax with  £500,000 (ico., 2020).

Equifax was also fined by the Financial Conduct Authority(FCA) which works to make market to run serviceably so that the customer gets good deal (Financial Conduct Authority, 2024). The quantum of the penalty was £11,164,400. Equifax Ltd. got a 30% reduction through the Authority’s executive settlement procedures by agreeing to resolve this disagreement. If Equifax Ltd. wasn't granted a 30% reduction on this penalty, they would be demanded to pay a penalty of £15,949,200 (FINANCIAL CONDUCT AUTHORITY, 2023).

A global agreement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and all 50 countries and homes of the United States claimed Equifax Inc. to pay at least$ 575 million and nearly $ 700 million. Also, Equifax stated that starting from January 2020, it'll give all American consumers six free credit reports for seven years, added on to the one yearly free credit report that it used to provide before the incident. Equifax was blamed for not taking necessary steps to protect its network which affected 147 million people. (FEDERAL TRADE COMMISSION, 2019).

# 4. SECTION 3: Chief Information Security Officer

If I was the CISO of the Equifax I would have done following tasks that might have prevented the incident

## 4.1. Proactive measures

Every time a company has an option, first to invest on the security solutions and second is to get ready to face the destruction and to get affected by every possible ways i.e. monetary, reputation etc. As, a CISO of a company I would have choose the first option performing the tasks given below:

1. Proper segmentation: The idea of dividing into many small parts to improve the security and performance is known as segmentation. It is also known as network isolation. It’s unclear whether Equifax used network segmentation. Properly segmenting networks limits the impact of a breach by restricting access to sensitive data even if hackers gain entry.
2. Modernizing Technology and Patching Systems: To maintain the company's security, I would have updated the technology and tools used by the organization. I would have made sure that systems were patched as soon as vulnerabilities were found. Equifax's failure to deal with this contributed to the hack.
3. Use of Web Application Firewall (WAF): I would have used the Web Application Firewall which protects systems exposed to the Internet from attacks based on the exploitations of web application-based security vulnerabilities.
4. Implement the principle of least privilege: I would have implemented the least privilege principle which commands that every entity in a system should be granted a minimum set of permissions to perform its designated tasks . In conjunction with compartmentalization, the least privilege principle can provide a finer grain for granting access to system components and prevent attackers from entering other parts of the system via elevated privileges on the compromised element.
5. Encrypt the data that resides in the system: I would have encrypted all the data that resided in the system. In a situation where the encrypted data is stolen but the encryption key is safe, then it is not said to be the data breach.

6. Implement IPS and IDS: IDS monitors the network. If any unwanted or harmful traffic is found, it alerts the logging and monitoring team based on mechanism configured to trigger the alert message. IPS also does the same task, but it does a additional work i.e. it stops all the susceptible network traffic till it is decided to let it flow again. I would have implemented these systems which would have helped to prevent or reduce the impact of the breach in the company.

### 4.2. Post-active measures

After, the incident I would have patch the vulnerable system as soon as possible. One of the reasons of a lot of data being breached is due to lack of proper segmentation. I would have focused on properly segmenting or isolating every database that resided in the system of the company. Despite being aware of the vulnerability, the company was not able to find the affected systems. Considering that I would have also focused on modernizing the tools and technologies of the system and implemented the defensive tools like IDS and IPS. I would have also purchased other applications and software too such as: antivirus, antimalware, WAF etc... Attackers can attack the system from many other methods than the method used in this incident so I would have provided every employee in the company with proper security training. Equifax had encrypted the communication channels only that were used to link the databases in the system but that came as a advantage for the attackers to insert queries while staying hidden. So, I would have encrypted every data that was stored in the system so that even if the data was stolen, they would not be readable without the proper decryption key.

The Equifax company had made many mistakes that led to this incident the harmed the company in every possible way. So, I would have properly studied all those factors to solve them effectively.

## 5. Conclusion

Security risks are rising in sync with technological advancements and the global shift from paper to digital media. The corporation Equifax, which is among the top three credit reporting agencies globally and is the topic of this study that suffered a data breach in 2017. Many data were leaked. The data included names, date of birth, social security number, address, driving license number and the dispute documents that included the PII. This incident occurred due to the vulnerability that was present in the Apache struts. Also, Equifax was not able to find the vulnerable system and patch it effectively. It didn't respond properly even after being aware of the vulnerability 2 months before the vulnerability was exploited.

After, thoroughly understanding the present scenario of the cyber-attacks and the case of the "Equifax data breach" we can conclude that nowadays an individual, company, organizations etc.… are not suffering from the physical robbers. They are suffering and are in danger due to the digital thieves and robbers. In present scenario data is money and nowadays maximum organizations prefer to save these data in the digital devices and cloud as well as. That increases the risk of losing the data causing the extreme harm to the company.

Proper modern tools and techniques such network and database segmentation, use of firewall, antivirus, imposing the zero-trust policy, implementation of the least privileges policy, encryption of data and use of IDS and IPS should be done to keep the system and organization as much secure as possible from the cyber threats and attacks. Most importantly CIA (Confidentiality, Integrity, Availability) triad should be maintained in a balanced. They work as the core pillar for the IT security. While maintaining one pillar, it should not harm another two, this should be considered while planning while creating a roadmap of the security in any organization.

Therefore, every organization that stores the data in the digital devices and uses networks and internet to communicate should strictly follow it security measures and try to be proactive to save themselves from being attacked and exploited by the attackers.

## 6. References

BBC, 2018. *Equifax fined by ICO over data breach that hit Britons.* [Online] Available at: https://www.bbc.com/news/uk-england-essex-45574163 [Accessed 29 march 2024].

Bracy, J., 2017. *The Equifax breach, response, and fallout.* [Online] Available at: https://iapp.org/news/a/equifax-data-breach-affects-143-million-consumers/ [Accessed 25 march 2024].

Brown, M., 2018. *One Year Later: The Impact of Equifax's Data Breach.* [Online] Available at: https://tdwi.org/articles/2018/10/29/biz-all-impact-of-equifax-data-breach.aspx
[Accessed 24 march 2024].

CISCO, 2024. *What Is a CISO?.* [Online] Available at: https://www.cisco.com/c/en/us/products/security/what-is-ciso.html [Accessed 1 april 2024].

CISCO, 2024. *What Is an Advanced Persistent Threat (APT)?.* [Online] Available at: https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html
[Accessed 15 4 2024].

equifax, 2017. *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes.* [Online]
Available at: https://investor.equifax.com/news-events/press-releases/detail/237/equifax-releases-details-on-cybersecurity-incident
[Accessed 25 march 2024].

equifax, 2023. *Driving the Global Economy Forward with Cloud Technology.* [Online] Available at: https://investor.equifax.com/company-information [Accessed 23 march 2024].

FBI, 2020. *Chinese Military Hackers Charged in Equifax Breach.* [Online] Available at: https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-

breach-021020#:~:text=According%20to%20the%20indictment%2C%20Wu%20Zhiyong%2C%20Wang%20Qian%2C,the%20dispute%20resolution%20website%20within%20the%20Equifax%20system.
[Accessed 1 may 2024].

FEDERAL TRADE COMMISSION, 2019. *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach.* [Online] Available at: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach
[Accessed 30 march 2024].

FINANCIAL CONDUCT AUTHORITY, 2023. *Final Notice 2023: Equifax Limited [pdf].* [Online]
Available at: https://www.fca.org.uk/publication/final-notices/equifax-limited-2023.pdf
[Accessed 30 march 2024].

Financial Conduct Authority, 2024. *About the FCA.* [Online]
Available at: https://www.fca.org.uk/about
[Accessed 15 4 2024].

Ford, N., 2024. *Global Data Breaches and Cyber Attacks in 2024.* [Online] Available at: https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024
[Accessed 21 march 2024].

Ford, N., 2024. *List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached.* [Online]
Available at: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
[Accessed 21 march 2024].

freebie supply, 2024. *Equifax Logo.* [Online]
Available at: https://freebiesupply.com/logos/equifax-logo/
[Accessed 20 may 2024].

geeksforgeeks, 2020. *Vulnerabilities in Information Security.* [Online] Available at: https://www.geeksforgeeks.org/vulnerabilities-in-information-security/ [Accessed 1 may 2024].

Google Cloud, 2020. *What is encryption?.* [Online] Available at: https://cloud.google.com/learn/what-is-encryption [Accessed 1 may 2024].

GOV.UK, n.d. *About us.* [Online] Available at: https://www.gov.uk/government/organisations/information-commissioner-s-office/about
[Accessed 1 may 2024].

Government Accountability Office (GAO), 2024. *DATA PROTECTION: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* s.l.: Government Accountability Office (GAO).

hackerone, 2024. *Information Security Policy: Examples and 11 Elements of a Successful Policy.* [Online] Available at: https://www.hackerone.com/knowledge-center/information-security-policy [Accessed 1 april 2024].

HAYES, A., 2022. *Federal Trade Commission (FTC): What It Is and What It Does.* [Online] Available at: https://www.investopedia.com/terms/f/ftc.asp [Accessed 1 may 2024].

ico., 2020. *Who we are.* [Online] Available at: https://ico.org.uk/about-the-ico/who-we-are/ [Accessed 30 march 2024].

International Energy Agency (IEA), 2020. *Significant cyber incidents worldwide, 2006-2019.* [Online] Available at: https://www.iea.org/data-and-statistics/charts/significant-cyber-incidents-worldwide-2006-2019
[Accessed 29 march 2024].

Jackie Wattles, S. L., 2017. *How the Equifax data breach happened: What we know now.* [Online]
Available at: https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html
[Accessed 25 march 2024].

john, A. S., 2017. *Equifax Data Breach: What Consumers Need to Know.* [Online]
Available at: https://www.consumerreports.org/electronics-computers/privacy/what-consumers-need-to-know-about-the-equifax-data-breach-a1040025441/
[Accessed 24 march 2024].

kaspersky, 2024. *What is Cyber Security?.* [Online]
Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
[Accessed 21 march 2024].

Malwarebytes, 2024. *SQL injection.* [Online]
Available at: https://www.malwarebytes.com/sql-injection
[Accessed 1 may 2024].

Marsh Commercial, 2022. *What should you do if your business is hacked?.* [Online]
Available at: https://www.marshcommercial.co.uk/articles/your-business-hacked/
[Accessed 1 march 2024].

Microsoft, 2022. *What is a Cyber-Attack & How Can I Protect Myself?.* [Online]
Available at: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-a-cyber-attack-how-can-i-protect-myself
[Accessed 1 april 2024].

Miyashiro, I. K., 2021. *Case Study: Equifax Data Breach.* [Online]
Available at: https://sevenpillarsinstitute.org/case-study-equifax-data-breach/
[Accessed 24 march 2024].

Oracle, 2020. *What Is a Database?.* [Online] Available at: https://www.oracle.com/database/what-is-database/ [Accessed 1 april 2024].

Royal Canadian Mounted Police, 2021. *Have you been a victim of cybercrime?.* [Online] Available at: https://www.rcmp-grc.gc.ca/en/have-been-a-victim-cybercrime [Accessed 29 march 2024].

Walsh, C., 2024. *Financial Conduct Authority (FCA) – Everything You Need to Know.* [Online]
Available at: https://moneyadvisor.co.uk/financial-conduct-authority/ [Accessed 1 may 2024].

Yasar, K., 2024. *firewall.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/firewall [Accessed 1 april 2024].

# 7. Appendix

## 7.1. Fine imposing bodies

### 7.1.1. FTC (Financial Trade Commission)

It is an independent organization of U.S government established in 1914 whose main aim is to carry out the civil (non-criminal) antitrust law and promote consumer protection from predatory or misleading business practices. It's regular activity is to look over the fraud, incorrect broadcast from costumers, establishments, media, pre-merger notification and congressional inquiries. It's headquarter is located in in Washington, DC (HAYES, 2022).

### 7.1.2. FCA (Financial Conduct Authority)

It is the UK's financial supervisory authority in U.K that supervise over 51,000 firms to maintain the integrity and fairness in the U.K financial market. FCA is controlled by U.K legislation and works within a structure set by it. It mainly works under the law such as Financial Services and Markets Act 2000. The structure set by the legislation makes sure that it works while maintaining the transparency and accountability (Walsh, 2024).

### 7.1.3. Information commissioner's office

The information commissioner's office supports the information right of the public by publicizing the transparency of the government agencies and data privacy of individual. They take the disagreements and take the suitable actions if any entity breaks the law. They also counsel the individuals and the establishments (GOV.UK, n.d.).

### 7.2. who were suspected?

In February 10, four Chinese army were charged for having connection with the data breach that occurred in Equifax in 2017, by U.S. Department of justice that is globally known as the largest theft of Personally Identifiable information. A multinational investigative group that was led by FBI's Atlanta Field Office was formed to find the person behind this attack. They followed the digital footprint of the crime and found that the attackers used 40 diverse IP address to hide their original location. Wu Zhiyong, Wang Qian, Xu Ke and Liu Lei were suspected of the exploitation of the Vulnerability in Apache struts tht was housing the online dispute portal of Equifax (FBI, 2020). More details on this topic are given in the link given below:

https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020#:~:text=According%20to%20the%20indictment%2C%20Wu%20Zhiyong%2C%20Wang%20Qian%2C,the%20dispute%20resolution%20website%20within%20the%20Equifax%20system.