



CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Spring

Credit: 15 Semester Long Module

Student Name: Aayush Raj Kafle

London Met ID: 23047570

College ID: NP01NT04A230231


Assignment Due Date: Saturday, April 19, 2025

Assignment Submission Date: Monday, May 19, 2025

Word Count: 3444

I confirm that I understand my coursework needs to be submitted online via MySecondTeacher 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 mark of zero will be awarded.

23047570 Aayush Raj Kafle.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid:::3618:96631727

Submission Date

May 19, 2025, 11:54 AM GMT+5:45

Download Date

May 19, 2025, 11:55 AM GMT+5:45

File Name

23047570 Aayush Raj Kafle.docx

File Size

21.7 KB

21 Pages

3,444 Words

18,568 Characters



Page 1 of 24 - Cover Page





Submission ID trn:oid:::3618:96631727

Figure 1 Similarity report page 1




1% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **1 Not Cited or Quoted 0%**
Matches with neither in-text citation nor quotation marks
-  **1 Missing Quotations 0%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 1%  Internet sources
- 0%  Publications
- 0%  Submitted works (Student Papers)

Integrity Flags





0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.




A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Figure 2 Similarity report page 2

Match Groups

-  **1 Not Cited or Quoted 0%**
Matches with neither in-text citation nor quotation marks
-  **1 Missing Quotations 0%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 1%  Internet sources
- 0%  Publications
- 0%  Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

<div>1 Submitted works</div>		
American College of Education on 2023-01-12		<1%
<div>2 Internet</div>		
www.absolutemarketsinsights.com		<1%

Figure 3 Similarity report page 3

Abstract

This report will analyse the 2019 Capital One data breach, a significant cybersecurity incident resulting from a misconfigured web application firewall within their Amazon Web Services (AWS) environment. The breach, perpetrated by a former Amazon employee exploiting a Server-Side Request Forgery (SSRF) vulnerability, compromised the personal information of over 106 million individuals. This analysis delves into the technical misconfiguration that enabled the breach, the roles of Capital One and the attacker, and the ensuing ethical, social, professional, and legal ramifications faced by the financial institution, drawing upon ethical frameworks outlined in Sara Baase's "A Gift of Fire." The findings underscore the critical importance of robust cloud security practices, timely breach disclosure, and adherence to ethical and legal responsibilities for organizations handling sensitive consumer data, serving as a stark reminder of the far-reaching consequences of neglecting cybersecurity best practices in the cloud era.

Table of Contents

1.	Introduction.....	1
1.1	Background.....	2
2.	Social Issues.....	4
2.1)	Failure in Timely Disclosure	4
2.2)	Privacy & Security Issues	4
2.3)	Public Concern Over Cloud Security.....	4
2.4)	Erosion of Public Trust in Capital One.....	5
2.5)	Psychological Distress	5
3.	Ethical Issues	6
3.1)	Failure to Prioritize People Over Company.....	6
3.2)	Distress to Consumers.....	6
3.3)	Lack of proper Data protection	7
3.4)	Delay in disclosure about the breach	7
3.5)	Storage of unauthorized personal Details	8
4.	Legal Issues.....	9
4.1)	OCC Settlement (2021).....	9
4.2)	Class-Action Lawsuits	9
4.3)	Criminal Prosecution of the Hacker.....	10
4.4)	Ongoing Compliance Requirements	10
4.5)	Regulatory Scrutiny and Enhanced Oversight.....	10
5.	Professional Issues	11
5.1)	Violation of ACM Code.....	11
5.2)	Operational Disruptions	11
5.3)	Vendor & Partner Distrust	12

5.4)	Executive Accountability	12
5.5)	Delay in knowing about the Breach.....	12
6.	Conclusion	14
7.	Personal reflection	15
8.	References.....	19
9.	Appendix.....	25
9.1)	Technical Terminology	25
9.2)	Aftermath	25
9.3)	Timeline Of the breach	27
9.4)	Similar Breaches	28
9.5)	Prevention Measures.....	28

Table of Figure

Figure 1 Similarity report page 1	1
Figure 2 Similarity report page 2	2
Figure 3 Similarity report page 3	3
Figure 4 How the attacker got in (Issa, 2020).....	2
Figure 6 Email Sent by a GitHub user notifying of the stolen data dump (Ma, 2019).....	12
Figure 7 Stock price before and after the announcement (yahoo finance, 2019)	25
Figure 8 Stock price one month after the breach (yahoo finance, 2019).....	26
Figure 5 Timeline of the breach.....	27
Figure 9 Graph of Similar breaches	30

1. Introduction

Capital One was established on July 21, 1994, by Richard Fairbank. Capital One was built with a mission to help customers succeed by bringing ingenuity, simplicity, and humanity to banking sector. (Capital One, 2025)

The organization was hit with a massive data breach in March of 2019, and it was not discovered till July of 2019. Capital One released the news 12 days after initial knowledge about the breach. The perpetrator was a former Amazon employee Paige Thompson who utilized the misconfigured WAF in Capital One's AWS to access their consumers data who applied for credit card from 2005 till 2019 (Capital One, 2022) and dump it into GitHub under the alias erratic. The breach leaked the details of more than 106 million consumers of Both US and Canada (Mandnick, 2022).

The report will be primarily focusing on the misconfiguration in EC2 that allowed Thompson to access S3 bucket and leak consumers data and figure out the fault of Capital One and Thompson's roles in the breach while discussing Ethical, Social, Professional and legal issue faced by Capital One according to Sara Baase Book A gift of Fire.

1.1 Background

The breach highlighted a critical vulnerability in cloud services if configured incorrectly as seen in this leak a misconfigured WAF allowed Thompson to utilize SSRF vulnerability to ensure server-side application makes requests to an unintended location (PortSwiggers, 2025).

Late night of 29th July 2019 Capital One held a press conference and announced to the public that their AWS was breached and many of their consumers around 106 million to exacts personal details were compromised (Jones, 2022). Capital One also begin to work with federal law enforcement related to that matter to minimize damage and arrest the perpetrator (capitalone.co, 2019).

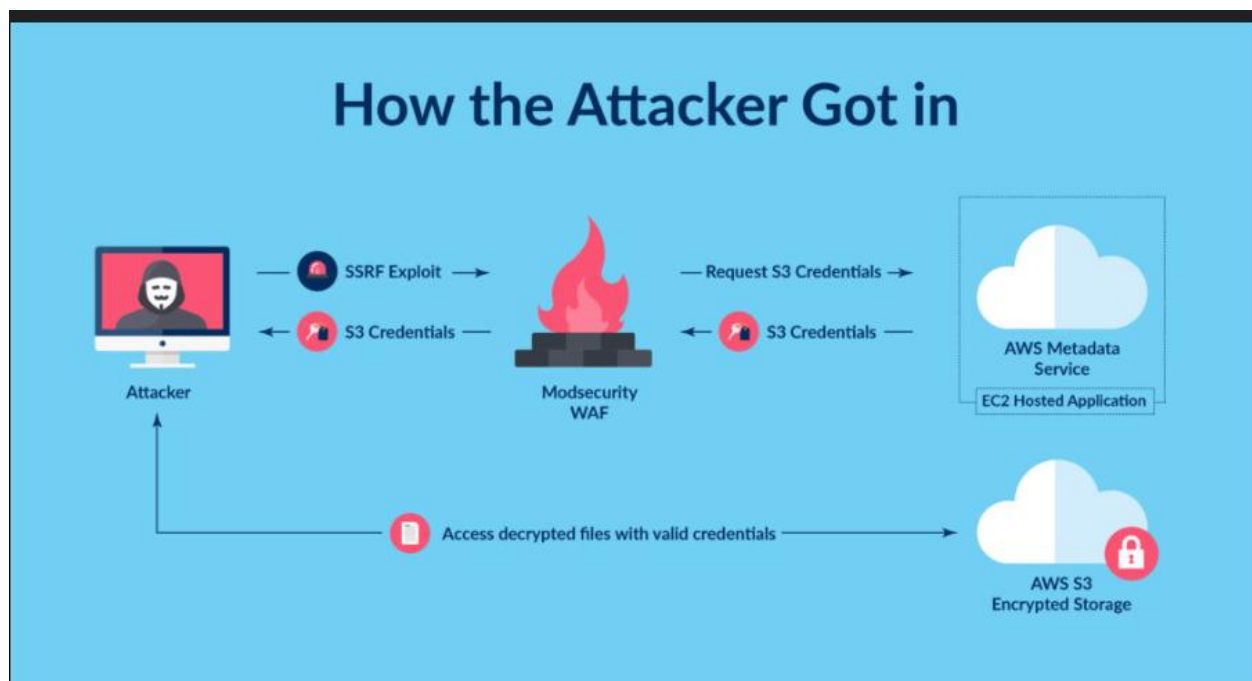


Figure 4 How the attacker got in (Issa, 2020)

Thompson Familiar with the AWS environment gained access to S3 buck and accessed consumers. Attacker used SSRF which allows attacker to exploit server resource (Kirk, 2019), it exploit within EC2 instance by bypassing WAF. Using this flaw attacker got S3 access to obtain credential by tricking appellation into making internal request to AWS mandate Service. After manipulating the service, she gathered all the sensitive data stored within AWS service (Kirk, 2019). She was found guilty of wire fraud and hacking charges by the Seattle jury (Kate Conger, 2022).

2. Social Issues

Misconfiguration of WAF EC2 instance allowed the threat actor to gain and steal Capital One database which allowed rise for criminals to conduct identity theft of the affected individuals which was more than 106 million. This also caused irreversible damage to Capital One's public image as some consumers were rightfully scared about the damage it was about to cause to their future as well as any decision in the future. Some social issues created by the Capital One breaches are :

2.1) Failure in Timely Disclosure

As a public organization, Capital One had a responsibility to promptly notify affected customers upon discovering a data breach. However, the company delayed alerting consumers for months, violating FTC transparency guidelines and increasing risks for millions. The delay allowed hackers more time to exploit stolen Social Security numbers and banking details. This incident highlights systemic flaws in corporate breach response policies, emphasizing the need for stricter regulatory enforcement to ensure timely consumer notifications in future cybersecurity incidents.

2.2) Privacy & Security Issues

The breach exposed sensitive data including Social Security numbers, bank details, and personal information of over 100 million Capital One customers. As Sara Baase argues, such large-scale privacy violations cause irreparable harm, leaving victims vulnerable to prolonged identity theft and fraud. Unlike credit cards, Social Security numbers are permanent, forcing affected individuals into lifelong credit monitoring. This incident highlights the dangers of lax data security and underscores the need for stronger firewalls, access controls, and regulatory oversight to protect consumer privacy.

2.3) Public Concern Over Cloud Security

Paige Thompson took advantage of a poorly configured AWS firewall, prompting widespread concern over cloud security. In the fallout, both businesses and consumers called into question the viability of cloud-based financial services, with surveys citing a

sharp loss of confidence. Capital One's breach in 2019 was a wakeup call that prompted business to start more strictly managing their cloud access and manage their firewall with even more strictly. This breach also speed industries to move toward Zero Trust Architecture security model and aggressively push toward compliance with cloud infrastructure. (Fier, 2019)

2.4) Erosion of Public Trust in Capital One

Thompson exploited a misconfigured WAF, severely damaging trust consumers had in Capital One and the broader banking sector. Studies show many customers reduced online banking activity due to security fears. Regulators fined Capital One of \$80 million to regulatory bodies like the OCC (Schroeder, 2020). The company was held liable for the breach and was ordered to pay \$190 million USD in the class-action lawsuit against them (Ennis, 2023) and U.S. Office of the Comptroller of the Currency also fined the organization 80 million USD for failure to properly configure their Waf in AWS services. (Rautmare, 2020).

2.5) Psychological Distress

The breach affected more than 100 million individuals after they applied for Capital One's Credit card and their information was stored without any proper safeguarding method. The emotional distress as due to the data breach they were in constant fear that they in a possibility that their data could have been stolen and sold to anyone with a malicious intent to cause them financial and legal harm .

3. Ethical Issues

Capital One neglected many concern and disregarding ethical duties of an organization to fulfil their financial gains by delaying the release about the breach by 10 days (capitalone.co, 2019) which could have allowed people to prepare. The breach also highlighted many of ethical issue raised by capital one before and during the breach. Some of the ethical issue raised during the breach are:

3.1) Failure to Prioritize People Over Company

According to Utilitarianism, an organization should care about prioritizing people but their action during the breach highlighted that they were more focused on minimizing people's reaction to the breach rather than proactively caring for the relationship between the consumer and the financial institution. In Ethics of Care (Relational Ethics) it says to focus on empathy and compassion disregarding rules to protect others (Gilligan, 2011).

3.2) Distress to Consumers

Virtue Ethics primarily focuses on the virtue honesty, integrity, empathy, and responsibility of any entity. In this case, the organization's action resulted in distress to millions of individuals due to carelessness. The company was not able to maintain its stored data and delayed disclosing about the breach which goes against the virtue theory of acting. Capital One's handling of the breach reflected carelessness in data protection. A virtuous organization would have prioritized consumer well-being by taking proactive security measures rather than correcting their mistakes. The lack of regard for such ethics also deepens the consumers' distress and demonstrates how such blatant disregard harms a cooperative organization.

3.3) Lack of proper Data protection

The news about the misconfigured WAF in Capital Ones AWS was the main reason Paige Thompson, a former Amazon Software Developer, was able to gain access to the S3 bucket and leak the consumers' details. Even though she was a former Amazon employee no one other than authorized individuals should have been able to access the S3 bucket. In the Deontological it says that an action is ethical if they follow rules and duties but capital one failed to follow those rules and lacked in properly doing their duties when they misconfigured firewall in the AWS which was among the core component of their organization. The lack of proper configuration shows capital Ones blatant disregard for Deontological Ethical Theory.

3.4) Delay in disclosure about the breach

According to the Utilitarianism theory which states that an action should be done in order to maximize happiness and reduce harm done to a minimum for the greatest number of people that are to be affected (Mill, 1863). In of Capital One case of 2019 the world saw that the organization delayed releasing news about the leak to the general public due to the fear of losing face and also losing trust among shareholders as the news about the scandal dropped the share value of the organization within the next day of making the news about the breach public (Imbert, 2019). The lack of concern for the public by delaying the news created some serious financial trouble for the affected individuals . If the organization had disclosed the information the day, they had discovered it would have allowed the affected consumers to protect themselves by locking their credit and monitoring it for any threats earlier. The action of delaying the news goes against the utilitarianism theory.

3.5) Storage of unauthorized personal Details

The Capital One Financial Organization stored information of millions of consumers from 2005 to 2019 that was taken by those who required credit cards from the financial Institution. We saw during the breach that the cooperation also violated Natural Rights Theory which says that action should always respect other individual rights and boundaries. The company failed to maintain the rights of their consumers when they failed to properly configure the firewall in the AWS which led to the leak. The company was responsible for the disregard for the individual rights of their consumers and for disregarding the Natural Rights Theory. If an organization stores others sensitive information, then they become responsible for the protection of those data. Some may argue that the cooperation stored data that was more than needed which also caused some uproar among the public.

4. Legal Issues

The breach caused many legal problems for both the capital one financial cooperation as well as the one who breached the AWS and took the details of the consumers like their personal details and financial information.

4.1) OCC Settlement (2021)

Due to the breach, Capital One was made to pay the fine of \$80 million to settle federal charges. OCC also claims that Capital One financial institution failed to implement proper cyber security measures as result millions of people were left vulnerable due to the breach. Gramm-Leach-Bliley Act is a safeguard rule made by the FTC that mandates companies to ensure their information security programs are developed, implemented and maintained with proper Administrative, technical, and physical safeguarding that will protect the consumers data (FTC, 1999), and capital one also failed to follow the act as a result FTC forced the company to improve upon their security measures by increasing regulatory scrutiny (Gaurav, 2025).

4.2) Class-Action Lawsuits

When the news about the breach came to the light many people were afraid of being affected by the breach which caused a law firm named Charney Lawyers PC to file a class action lawsuit against capital one on behalf of all affected Canadian citizen (Charney Lawyers PC, 2024). The Settlement included out of pocket 25,000\$ per person if they had receipts, Compensation for lost time which was up to 15 hours for 25\$/hr and an ongoing identity protection that will be ongoing till 2028 and 75–\$250 for those who still submitted valid claims but didn't file any documentation (Aijaz, 2025).

4.3) Criminal Prosecution of the Hacker

Not only did the organization come under scrutiny but the person Paige Thompson who was responsible for the breach also came under scrutiny. Thompson was a former Amazon employee, so it was easier for her to exploit the AWS misconfiguration due to her experience in the field (Broustail, 2022). She has been convicted by a federal jury and been sentenced to serve time and 5-year probation that includes location and computer monitoring of her till the end of probation by the U.S. District Court in Seattle (US attorney Office Western District Office, 2022). She used to go by the alias "erratic" through which she leaked the data on the public network.

4.4) Ongoing Compliance Requirements

Due to the Class action lawsuit against Capital One which was conducted after the organization announced that they will notify the affected consumers of the breach and offer them free of charge credit monitoring Services. Many Law firms like Morgan and Morgan law firm have joined to file a lawsuit against Capital One Organization on behalf of the affected consumers (Morgan, 2022). According the ruling in the lawsuit Capital One had to pay for consumers credit score Security and monitoring with identity monitoring with authentication alert and Capital One also provided 1 million\$ in third party insurance that covered cost related to cases like identity theft and fraud (Richie, 2022).

4.5) Regulatory Scrutiny and Enhanced Oversight

Following the breach of Capital One confidential information they had to face regulatory fines from multiple government and regulatory bodies that oversee the day-to-day operations conducted by financial organization. The OCC fined Capital One a total of 80 Million dollar in Monetary Penalty for their failure to properly establish a proper effective procedure for risk assessment before migrating their operation onto a cloud environment and also for failure to rectify their shortcoming in a timely ordinance (OCC, 2020). Although no further penalties were imposed many US states considered a possibility of strengthening existing data breach laws (Li, 2019)

5. Professional Issues

The massive breach that affected the 106 million users and consumers of Capital One triggered a huge professional consequence which were not limited to financial repercussion and ethical & social backlash from the public and the media. Some of the professionals that arose from the breach are:

5.1) Violation of ACM Code

Capital One violated ACM Code 2.1, IEEE Canon 1, BCS Section 1a, and SE Code 5.01 which states that computing professionals should avoid harm to others, including users, colleagues, and the public (ACM, 2018). Capital One instead of working with the ACM code they neglected in its proper application and because of that action millions of their consumers were in constant fear of being a victim of Identity fraud and having their future in a problematic situation.

5.2) Operational Disruptions

Due to the breach the misconfiguration of AWS came to light. After the breach Capital One had to divert funds and experts from both inside and outside the organization to fix the issues. Due to the rerouting of necessary monetary fund and skilled professionals to fix the AWS vulnerability Capital One had an disturbance in their work flow. Not only that many news channels published articles about how to freeze credit following the breach due to the risk of someone stealing the identity and misusing their financial condition for their own personal gain (Picchi, 2019). Due to freezing their credit cards, it affected mostly those who only had one or two credit card providers as it limited their choice for payment, disrupting their day-to-day activity.

5.3) Vendor & Partner Distrust

The breach amplified people distrust toward cloud services and demanded stricter cloud security assessment while using third part system. Some vendors fearing bad publicity added stricter security assessment policy before integrating into the cloud. Amazons were also blamed for the breach as SSRF breach as it was addressed by Amazon's competitors years ago, they continued to sell defective cloud computing services to multiple organizations. Paige Thompson, who was responsible for the breach, was also a former AWS employee (O'Donnell, 2019)

5.4) Executive Accountability

Following the breach news being disclosed to the public, the shareholders and the media heavily criticized the CEO and CISO for failing to prevent such disaster. The organization replaced their Cybersecurity chief 4 months after the news of the breach was made public. Michale Johnson who CISO during the breach was demoted to the Senior Vice role alongside managing the cyber security as the senior adviser (Whittaker, 2019). However, the CEO Richard Fairbank remained as the CEO and chairman post breach.

5.5) Delay in knowing about the Breach

The incident occurred on March 22nd and 23rd of 2019 but the breach was not discovered till 19th of July 2019 (Madnick, et al., 2020). The breach took almost 4 months and even then, it was thanks to an outsider, a GitHub user who notified Capital One if their Stolen data dump regarding their credit-card applicants' details being leaked (Ma, 2019).

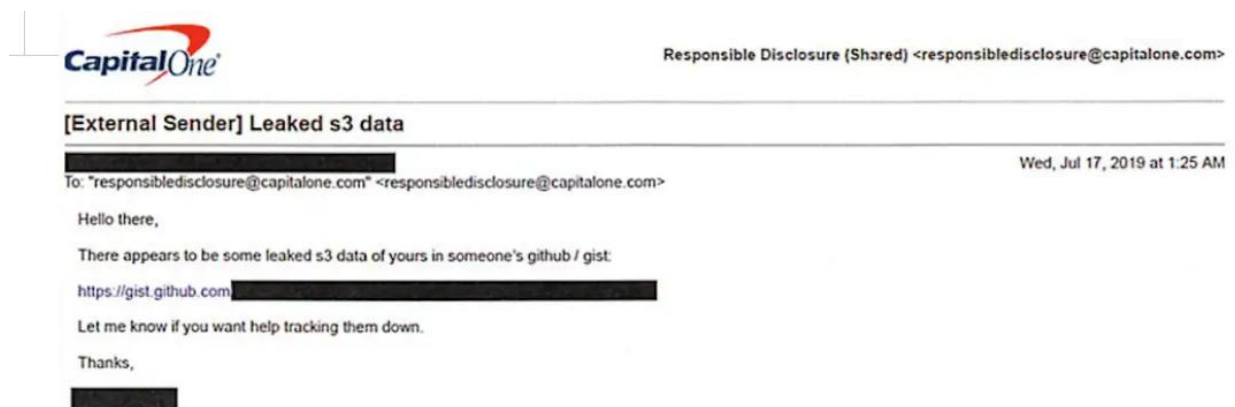


Figure 5 Email Sent by a GitHub user notifying of the stolen data dump (Ma, 2019).

The main issue in this case the lack of any security protocols like regular monitoring and the blatant disregard for the consumers personal data protection. If the External source had not notified the Capital one of the stolen data, it would had been in the GitHub for even a longer period and a malicious user could have used it for any kind of malicious activity. This showed a lack of professionalism rom Capital One in Data protection security measures

6. Conclusion

The breach not only affected the organization but had a chain reaction as multiple local bodies thought to toughen up on the cybersecurity related policy and eroded public trust and raised some concern about the organization. 2019 Capital One data breach of millions of their clients and was marked as one of the most significant cybersecurity incidents in financial history.

A former Amazon Software developer Paige Thompson who also goes by the alias 'ericaite' online stole the personal information and SSN of 100 million US based Capital Ones client by exploiting a misconfigured WAF in the cloud service causing mass panicky among affected individual and media outlet. The breach showed critical flaws in the cloud security of an international and large financial institution such as Capital One. The aftermath of the breach left the affected individual fear for their financial security, actions taken against Capital One by both the affected individuals and the regulatory bodies for failure to maintain basic standards, Criminal prosecution against Paige Thompson, backlash from the media and the public causing stock value to depreciate, and heavy reforms made to the cloud services used by Capital One.

7. Personal reflection

As the 2019 breach in Capital One's S3 bucket, a clear lack of regard was seen in Cloud Security by the Capital One Cybersecurity team and Capital One's CISO Michael Johnson while configuring WAF as it is one of the crucial steps in protection of cloud architecture services used by an organization.

Brain Storming

1. Affected Entities

a. Shareholders

The shareholders had to lose their invested money due to the breach

b. Capital One

The organization lost trust that the public and the investors had in them

c. Consumers

Were in constant fear for their financial wellbeing and were vulnerable to finance related fraud.

d. Governing bodies

OCC had to step in to minimize the impact of the breach and fine Capital One also FBI had to get involved to arrest Paige Thompson.

e. AWS

As the organization related to the breach Amazon was also affected.

2. Risks, Issues, Problems, and Consequences

a. Financial Losses

Capital One faced fines of \$80 Million, give free credit monitoring the affected individuals \$190 million lawsuits and invest in bettering their security to prevent similar incidents in the future. .

b. Identity Theft & Fraud

Exposed SSNs of the Capital One consumers, bank account details, and credit scores increased fraud risks.

c. Reputation Damage

Loss of customers and investors trust in Capital One and cloud security as well as backlash from the media.

d. Legal & Regulatory Consequences

Capital One faced Investigations, penalties, and stricter compliance requirements from the financial governing body (OCC).

e. Increased Cybersecurity Costs

Companies, mainly finance-related companies, started investing more in cloud security to prevent mistakes that were made by capital one.

3. Benefit

a. Improved Security Measures

Due to the after-breach effect, any future customer will benefit from stronger protection acts developed during the breach.

b. Legal Precedents: Regulatory bodies clarified even in more depth relating to cloud related action such as responsibility and security. .

c. Cybersecurity Industry Growth:

The breach created a domino effect that increased the demand from cybersecurity firms and ethical hackers to go defensive.

Analysis Phase

1. Responsibility

a. Capital One's Responsibility:

Before: Protect customer, data and comply with laws

During: Notify affected parties and the relevant governing bodies

After: Rectify the error to prevent similar problems in the future.

b. Customers' Rights:

Privacy, transparency, compensation for damages after being affected from the breach accordingly to the damage caused to them.

c. Regulators' Role: E

Before: Enforce laws and conduct regular audits in a timely manner.

During: Arrest the perpetrators.

,After: Penalize the one who caused the breach and protect consumers.

2. Affected Code

ACM Code 1.2: Avoid harm (breach harmed millions).

SE Code 2.03: Maintain integrity and privacy of data.

SE Code 3.12: Ensure proper system security measures

3. Action categorization

a. Ethical Obligatory:

Capital One should notify customers in proper time

Improving security in their AWS to prevent breaches

b. Ethical Prohibited:

Ignoring the cause of the breach

Hiding the extent of the breach.

Delay notifying the affected parties

c. Ethical Acceptable

Offering credit monitoring

Competition according

Payment of fines and lawsuit

Improvement in cloud security.

Final Thoughts

Looking past into the breach there were many vulnerabilities that were ignored which later turned into a serious issue even though with adequate management and strengthen the policies could have prevent such a disaster. Some of the issues that Capital One had to face and their solutions are given as follows:

1. Full transparency
Discloser breach details promptly after gaining knowledge about their existence
2. Investing in stronger cloud security
prevent recurrence that helps in avoiding the issues
3. Compensating affected users
Credit monitoring
Fraud protection).
4. Regulatory reforms
Having stricter Cloud security protocols and investing in better cyber and cloud security

8. References

Aijaz, D., 2025. *\$190M Capital One Data Breach Settlement: What Really Happened?*. [Online]
Available at: <https://www.purewl.com/capital-one-data-breach-settlement/>
[Accessed 19 04 2025].

Bowie, N. E., 2017. *Business Ethics: A Kantian Perspective*. 2nd ed. Minnesota: Cambridge University Press.

Broustail, A., 2022. *Ex-AWS engineer convicted of hacking data of 100 million customers*. [Online]
Available at: https://www.business-standard.com/article/companies/ex-aws-engineer-convicted-of-hacking-data-of-100-million-customers-122061900275_1.html
[Accessed 19 04 2025].

Capital One, 2022. *Capitalone.com*. [Online]
Available at: <https://www.capitalone.com/digital/facts2019/>
[Accessed 26 3 2025].

Capital One, 2025. *About Us*. [Online]
Available at: <https://www.capitalone.com/about/corporate-information/our-company/>
[Accessed 12 5 2025].

capitalone.co, 2019. *Capital One Announces Data Security Incident*. [Online]
Available at: <https://investor.capitalone.com/news-releases/news-release-details/capital-one-announces-data-security-incident>
[Accessed 26 03 2025].

capitalone.co, 2019. *Capital One Announces Data Security Incident*. [Online]
Available at: <https://investor.capitalone.com/news-releases/news-release-details/capital-one-announces-data-security-incident>
[Accessed 28 02 2025].

Charney Lawyers PC, 2024. *Capital One Class Action*. [Online]
Available at: <https://www.charneylawyers.com/capital-one-privacy-breach-class-action/home>
[Accessed 19 04 2025].

Ennis, D., 2023. *Fed ends Capital One breach-related enforcement action*. [Online] Available at: <https://www.cybersecuritydive.com/news/fed-ends-capital-one-breach-action/686970/#:~:text=Capital%20One%20in%20December%202021,customers%2C%20according%20to%20bank%20estimates.>

[Accessed 07 04 2025].

Ennis, D., 2023. *Fed ends Capital One breach-related enforcement action*. [Online] Available at: <https://www.cybersecuritydive.com/news/fed-ends-capital-one-breach-action/686970/>

[Accessed 16 04 2025].

Fier, J., 2019. *Lessons from the Capital One Breach on Cloud Security*. [Online] Available at: <https://www.darktrace.com/blog/back-to-square-one-the-capital-one-breach-proved-we-must-rethink-cloud-security>

[Accessed 07 04 2025].

Fruhlinger, J., 2024. *Equifax data breach FAQ: What happened, who was affected, what was the impact?*. [Online]

Available at: <https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html>

[Accessed 16 04 2025].

FTC, 1999. *Gramm-Leach-Bliley Act*. [Online]

Available at: <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

[Accessed 19 04 2025].

Gaurav, 2025. *Capital One Data Breach Settlement 2025, Users Can Still Claim The Extra Services*. [Online]

Available at: <https://www.jetauj2023.com/capital-one-settlement-claim-deadline/>

[Accessed 19 04 2025].

Gilligan, C., 2011. *An Ethic of Care: A Relational Ethic for the Relational Characteristics of Organizations*. [Online]

Available at: <https://link.springer.com/chapter/10.1007/978-90-481-9307->

3 1#:~:text=In%20addition%20to%20these%20four,of%20the%20other%20or%20others.

[Accessed 26 04 2025].

Imbert, F., 2019. *Capital One shares dive after data breach affecting 100 million*. [Online] Available at: <https://www.cnbc.com/2019/07/30/capital-one-shares-dive-after-data-breach-affecting-100-million.html>

[Accessed 08 04 2025].

Issa, W., 2020. *How the Capital One breach could have been avoided with application-layer data encryption*. [Online]

Available at: <https://www.ubiqsecurity.com/how-the-capital-one-breach-could-have-been-avoided-with-application-layer-encryption/>

[Accessed 15 04 2025].

Jones, T., 2022. *Capital One Data Breach — 2019*. [Online]

Available at: <https://medium.com/nerd-for-tech/capital-one-data-breach-2019-f85a259eaa60>

[Accessed 27 03 2025].

Kate Conger, 2022. *Ex-Amazon Worker Convicted in Capital One Hacking*. [Online]

Available at: <https://www.nytimes.com/2022/06/17/technology/paige-thompson-capital-one-hack.html>

[Accessed 26 03 2025].

Kirk, J., 2019. *Capital One's Breach May Be a Server Side Request Forgery*. [Online]

Available at: <https://www.bankinfosecurity.com/capital-ones-breach-may-be-server-side-request-forgery-a-12871>

[Accessed 28 02 2025].

Li, Z., 2019. *The Status of Data Breach Law in Light of Capital One*, Boston: Boston University.

Ma, A., 2019. *Capital One found out about its 106-million-customer data breach only because a member of the public emailed it a tip.* s.l.: Business Insider.

Madnick, S., de Paula, A. M. G., Borges, N. M. & Neto, N. N., 2020. *A Case Study of the Capital One Data*, Las Vegas: Information Institute Conferences.

Mandnick, S. K. K. H., 2022. *A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned.* [Online]

Available at: <https://dl.acm.org/doi/10.1145/3546068>
[Accessed 12 04 2025].

Mill, J. S., 1863. *UTILITARIANISM.* [Online]

Available at: <https://www.utilitarianism.com/mill1.htm>
[Accessed 08 04 2025].

Morgan, M. &., 2022. *Was Your Personal Data Stolen? Join the Capital One Lawsuit.* [Online]

Available at: <https://www.forthethepeople.com/blog/was-your-personal-data-stolen-join-capital-one-lawsuit/>

[Accessed 21 04 2025].

OCC, 2020. *OCC Assesses \$80 Million Civil Money Penalty Against Capital One.* [Online]

Available at: <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html>
[Accessed 21 04 2025].

O'Donnell, L., 2019. *Is AWS Liable in Capital One Breach?.* [Online]

Available at: <https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/>
[Accessed 26 03 2025].

O'Donnell, L., 2019. *Is AWS Liable in Capital One Breach?.* [Online]

Available at: <https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/>
[Accessed 01 04 2025].

Panettieri, J., 2017. *Amazon AWS Cloud Data Leak: Accenture IP Exposed.* [Online]

Available at: <https://www.msspalert.com/news/amazon-aws-cloud-data-leak-accenture-ip-exposed>

[Accessed 16 04 2025].

Picchi, A., 2019. *How to freeze your credit following the Capital One breach.* [Online]

Available at: <https://www.cbsnews.com/news/freeze-my-credit-how-to-freeze-your-credit-in-the-wake-of-the-capital-one-breach/>

[Accessed 21 04 2025].

PortSwiggers, 2025. *Server-side request forgery (SSRF)*. [Online]
Available at: <https://portswigger.net/web-security/ssrf>
[Accessed 27 03 2025].

Rautmare, C., 2020. *Capital One Fined \$80 Million Over 2019 Breach*. [Online]
Available at: <https://www.bankinfosecurity.com/capital-one-fined-80-million-over-2019-breach-a-14787>
[Accessed 07 04 2025].

Richie, J., 2022. *Capital One Data Breach Class Action Settlement*. [Online]
Available at: <https://www.capitalonesettlement.com/en>
[Accessed 16 04 2025].

Schroeder, P., 2020. *Capital One to pay \$80 million fine after data breach*. [Online]
Available at: <https://www.reuters.com/article/business/capital-one-to-pay-80-million-fine-after-data-breach-idUSKCN2522D8/>
[Accessed 07 04 2025].

Schroeder, P., 2020. *Capital One to pay \$80 million fine after data breach*. [Online]
Available at: <https://www.reuters.com/article/business/capital-one-to-pay-80-million-fine-after-data-breach-idUSKCN2522D8/>
[Accessed 16 4 2025].

Stephen Gandel,CBS News, 2020. *Capital One to pay \$80 million fine for 2019 hack that exposed 100 million accounts*. [Online]
Available at: <https://www.cbsnews.com/news/capital-one-hack-credit-card-applications-settlement/>
[Accessed 27 03 2025].

Upguard Team, 2019. *Losing Face: Two More Cases of Third-Party Facebook App Data Exposure*. [Online]
Available at: <https://www.upguard.com/breaches/facebook-user-data-leak>
[Accessed 16 04 2025].

US Attorney Office , 2022. *United States v. Paige Thompson*. [Online]
Available at: <https://www.justice.gov/usao-wdwa/united-states-v-paige-thompson>
[Accessed 16 04 2025].

US attorney Office Wester District Office, 2022. *Former hacker sentenced for stealing computer power to mine cryptocurrency and stealing the personal information of more than 100 million people*. [Online]
Available at: <https://www.justice.gov/usao-wdwa/pr/former-hacker-sentenced-stealing-computer-power-mine-cryptocurrency-and-stealing>
[Accessed 19 04 2025].

Whittaker, Z., 2019. *Capital One replaces security chief after data breach*. [Online]
Available at: <https://techcrunch.com/2019/11/07/capital-one-security-chief-shuffle/>
[Accessed 21 04 2025].

Wong, J. C., 2017. *Uber concealed massive hack that exposed data of 57m users and drivers*. [Online]
Available at: <https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack>
[Accessed 16 04 2025].

yahoo finance, 2019. *Capital One Financial Corporation (COF)*. s.l.:yahoo!finance.

9. Appendix

9.1) Technical Terminology

1) OCC - Office of the Comptroller of the Currency

An independent bureau within the U.S. Department of the Treasury that is responsible for chartering, regulating, and supervising national banks and federal savings associations.

2) SSRF - Server-Side Request Forgery

A web security vulnerability where an attacker manipulates a web application to make requests on behalf of the server, potentially accessing internal resources or external systems that would otherwise be inaccessible to the attacker. This can lead to data breaches, information leaks, and even system compromise

9.2) Aftermath


Stock Price Decline

Due to the breach Capital had lost the trust tha their consumers had in them. Ust the day after the breach capital one lost 6.69% of their total share value (Imbert, 2019).

Date	Open	High	Low	Close 	Adj Close 	Volume
Jul 31, 2019	91.30	93.41	90.94	92.42	83.47	5,102,800
Jul 30, 2019	91.48	92.00	89.29	91.21	82.38	12,268,200
Jul 29, 2019	98.03	98.28	96.59	96.92	87.53	2,427,900
Jul 26, 2019	95.99	98.62	95.59	98.08	88.58	3,221,300
Jul 25, 2019	96.85	96.87	95.55	95.90	86.61	2,427,700
Jul 24, 2019	94.26	97.13	93.74	96.92	87.53	3,945,000
Jul 23, 2019	91.93	94.50	91.80	94.34	85.20	2,275,600

Figure 6 Stock price before and after the announcement (yahoo finance, 2019)

After the breach the value of the share kept on plummeting lower and lower reaching around 84.32 value per share and loosing around 14% of share value before the discloser about the breach. The organization was able to reach their previous share market value after around 3 months on Nov 7 , 2019.

My Portfolio	News	Markets	Research	Personal Finance	Videos	Streaming Now	
COF	Aug 28, 2019	82.76	84.86	82.67	84.59	76.73	1,818,500
Capital One Fina...	Aug 27, 2019	84.82	85.03	82.63	83.11	75.39	1,927,800
	Aug 26, 2019	83.55	84.32	83.15	84.28	76.45	1,428,900
171.50 +5.39% C	Aug 23, 2019	85.12	85.89	82.68	83.11	75.39	2,172,400
Summary	Aug 22, 2019	86.24	86.80	85.24	85.73	77.77	2,074,700
News	Aug 21, 2019	86.36	86.58	85.78	86.02	78.03	1,073,200
Chart	Aug 20, 2019	86.53	86.65	85.11	85.22	77.30	1,838,000
Conversations	Aug 19, 2019	86.85	87.45	86.25	86.97	78.89	2,066,400
Statistics	Aug 16, 2019	84.51	85.77	83.27	85.50	77.56	1,797,000
Historical Data	Aug 15, 2019	83.94	85.08	83.27	83.67	75.90	2,113,900
Profile	Aug 14, 2019	85.21	85.77	83.40	83.45	75.70	3,022,600
Financials	Aug 13, 2019	85.51	87.95	85.33	87.21	79.11	3,063,400
Analysis	Aug 12, 2019	86.65	87.09	85.31	85.69	77.73	1,983,000
Options	Aug 9, 2019	88.37	88.60	87.22	87.71	79.56	2,000,800
Holders	Aug 8, 2019	88.40	89.47	87.94	88.76	80.52	2,597,700
Sustainability	Aug 7, 2019	86.53	88.20	85.36	87.95	79.78	2,824,500
	Aug 6, 2019	87.15	88.42	85.89	88.30	80.10	2,810,000
	Aug 5, 2019	88.18	88.58	85.85	86.62	78.57	3,189,100
	Aug 2, 2019	0.4 Dividend					
	Aug 2, 2019	90.70	90.70	88.28	89.85	81.50	2,802,100
	Aug 1, 2019	92.42	93.65	91.07	91.30	82.46	3,517,000
	Jul 31, 2019	91.30	93.41	90.94	92.42	83.47	5,102,800
	Jul 30, 2019	91.48	92.00	89.29	91.21	82.38	12,268,200

Quote Lookup

Sign in to access your portfolio

Sign in

Top gainers

HTZ

Hertz Global Hol...

+2.51 (+43.07%)

8.22

CAR

Avis Budget Gro...

+11.90 (+16.37%)

84.59

LLY

Eli Lilly and Com...

+105.06 (+14.30%)

839.86

DIT

Trump Media & T...

+2.30 (+11.65%)

22.04

BMI

Badger Meter, Inc.

+17.73 (+9.64%)

201.63

Top losers

UNH

UnitedHealth Gr...

-130.93 (-22.38%)

454.11

GPN

Global Payments...

-14.66 (-17.43%)

89.46

SNA

Snap-on Incorpo...

-26.56 (-8.00%)

305.44

QXO

QXO, Inc.

-1.11 (-7.78%)

13.15

NVO

Novo Nordisk A/S

-4.80 (-7.63%)

58.08

Most active

NVDA

NVIDIA Corporat...

-3.06 (-2.93%)

101.43

Figure 7 Stock price one month after the breach (yahoo finance, 2019)

9.3) Timeline Of the breach

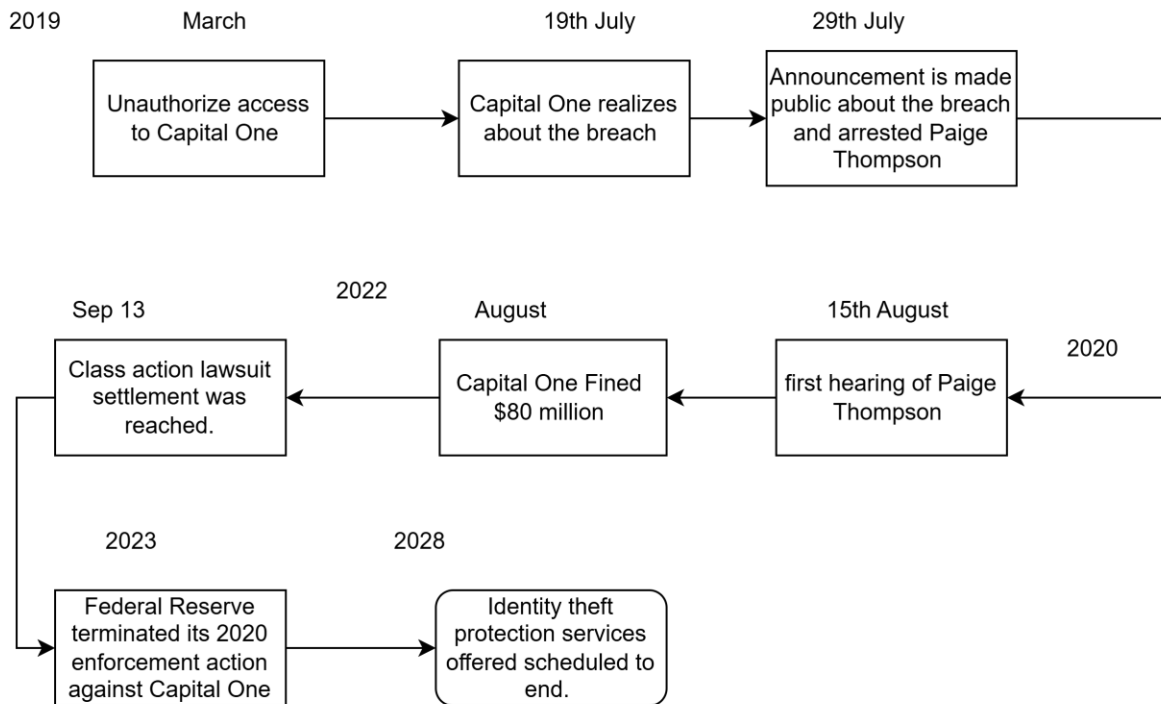


Figure 8 Timeline of the breach

In March of 2019 Paige Thompson got access to S3 of Capital where all the user credential were stored but Capital one only realized about the breach in 19th of July 2019 and released the new 10 days later and Paige Thompson was arrested on the same day (Ennis, 2023). She had on first court appearance on 15th August of the same year (US Attorney Office , 2022). Capital One \$80 million penalty to a U.S. bank regulator which was reported in August of 2020 (Schroeder, 2020). Class action settlement was reached in Sep 13 of 2022 where Capital One pay settlement to affected indivisibles (Richie, 2022). And finally in 2028 the settlement service provided by Capital One come to an end.

9.4) Similar Breaches

Capital One was not the only multinational organization that had a massive breach of more than 100 million individuals, spanning more than a country and faced multiple backlashes from media, public and regulatory bodies. There has been 5 similar breaches that closely resemble Capital One breach of 2019 in terms of cloud misconfigurations, insider threats, or large-scale data exposure:

- Equifax Data Breach 2017

In 2017 Equifax faced a breach which occurred in Apache Struts due to failure to patch a known vulnerability that caused 147 million individuals to be affected (Fruhlinger, 2024).

- Facebook (UpGuard Leak) – 2019

Like Capital One this breach was caused by a third party who stored their data on a misconfigured S3 bucket which affected over 540 million users (UpGuard Team, 2019).

- Uber Breach 2016

Hackers were able to get inside Uber's private GitHub repo and get their hands into credentials to gain access to S3 bucket and this breach affected 57 million users (Wong, 2017).

9.5) Prevention Measures

- 1) Prevention of SSRF vulnerability by implementing stronger policies.

If the organization was able to properly implement policies that states how a WAF should be configured and penalties that would be followed for the proper configuration was not properly implemented. This would have deterred people from delaying or ignoring the task and maintained the security of the cloud storage service to hold the details of Capital One's consumers.

- 2) Importance of Regular Security Audits & Penetration Testing

The breach could have been detected earlier or even prevented if Capital One had conducted frequent security audits and penetration tests. A well-structured audit would have identified the misconfigured WAF and SSRF vulnerability before an attacker

exploited it. Organizations must adopt a proactive security approach, routinely testing their cloud infrastructure for weaknesses rather than waiting for external threats to expose them.

3) Ethical Responsibility in Data Minimization

Capital One stored excessive consumer data, including Social Security Numbers (SSNs) and financial details, dating back to 2005. This violated the principle of data minimization, which states that organizations should only retain necessary data for the shortest time possible. Had Capital One implemented stricter data retention policies and purged outdated records, the breach's impact would have been significantly reduced.

4) Need for Faster Incident Response & Transparency

Capital One took four months to detect the breach and ten days to disclose it publicly. This delay worsened the damage, as affected individuals had less time to protect themselves from identity theft. Organizations must establish real-time monitoring systems and clear incident response protocols to ensure swift action and transparent communication with stakeholders.

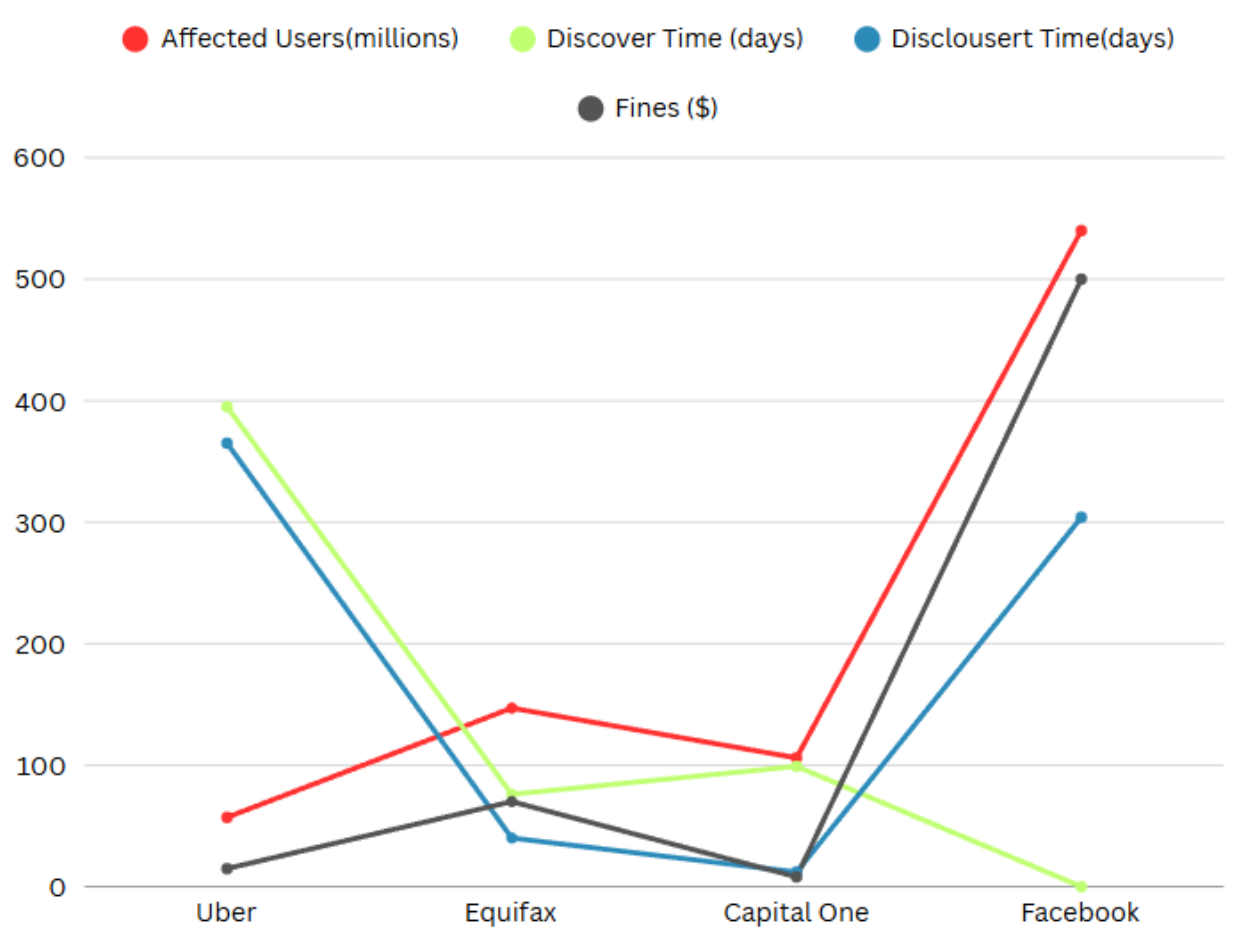


Figure 9 Graph of Similar breaches

The Graph shows the number of affected users, discovery and disclosure time and fines(10^7) of the companies that faced similar breaches. Uber's breach occurred in 2016 affecting 57 million users, took around 1 year to detect and another 14 to disclose about the breach and the company was fined 148 million. Equifax breach occurred in 2017 affecting 147 million users and was fined 700 million and the company took 40 days to disclose about the Breach after learning about the breach after around 2 and half months. Capital One took 12 days to disclose about the breach that occurs for around 00 days and affecting 106 million users, the financial intuition was fined 80 million dollars. Facebook breach occurred in 2019 and affected 540 million users, the detection date has not been disclosed but the breach information was released after 304 days after the detection and the company was fined 5 billion dollars.