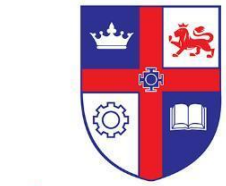
LONDON METROPOLITAN UNIVERSITY



islington college
(इस्लिङ्टन कलेज)

CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Spring

Credit: 15 Semester Long Module

Student Name: Bachan Timalsina

London Met ID: 23047401

College ID: NP01NT4A230100

Assignment Due Date: Monday, May 19, 2025

Assignment Submission Date: Monday, May 19, 2025

Word Count: 3420

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 marks of zero will be awarded.

Abstract

In 2019 Capital One experienced one of the biggest financial sector security breaches affecting more than 100 million individuals' personal and financial information. A misconfigured firewall inside a cloud environment triggered the breach that created major concerns about both social matters and ethical issues and legal problems and professional standards. The report starts by presenting an overview of the breach sequence and then it analyses the social repercussions which involve trust degradation and psychological distress. The research looks at ethical matters about privacy protection and transparency in relation to four key ethical frameworks including Deontology and Utilitarianism as well as Virtue Ethics and Rights Theory. The research identifies laws and regulations from U.S. and Canadian jurisdictions including bureaucratic penalties and criminal sanctions. The professional assessment of the breach focuses on ACM Code of Ethics standards which reveal missing points concerning competency and privacy matters and regulatory compliance requirements. The end of the document includes personal considerations which utilize ethical decision-making techniques to extract useful information about protecting cybersecurity in the future. Security practices together with ethical leadership and professional responsibility must have priority because of the essential need to protect digital information.

CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Spring

Credit: 15 Semester Long Module

Student Name: Bachan Timalsina

London Met ID: 23047401

College ID: NP01NT4A230100

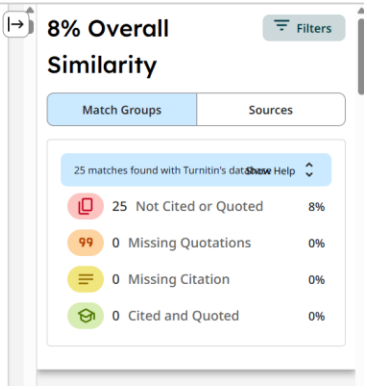


Table of Contents

Table of figures

1.Introduction

1.1 Introduction of the Company

Capital One is a significant financial company located in the United States, best recognized for its banking services, auto loans, and credit cards. As a tech-focused financial entity, Capital One significantly depends on digital frameworks, such as cloud computing, to handle customer information. Established in 1994, the company has expanded into one of the largest banks in the U.S., catering to millions of clients globally. Its embrace of cloud-based solutions intended to improve scalability, efficiency, and security. Nonetheless, this dependence on cloud technology brought about additional vulnerabilities, as demonstrated by the 2019 data breach (one, 2025).

1.2 Overview of modern Cyber Threats and Vulnerabilities

Cyber threats have evolved in complexity, impacting numerous sectors, particularly financial organizations. Typical online threats consist of:

Phishing Attacks – Fraudulent emails aimed at acquiring login information.

Ransomware – A type of malware that encrypts information and requests payment for decryption.

SQL Injection – Taking advantage of database weaknesses to obtain confidential data.

Insider Threats – Unauthorized entry by current or former employees.

Data Breaches – Unapproved disclosure of private information.

The Capital One incident is categorized as a data breach resulting from a misconfigured web application firewall, which granted unauthorized access to customer data.

2. Background of the Scandal

2.1 Overview of the Scandal

In March 2019 Capital One detected an unauthorized person stealing sensitive customer data due to device protection error on their servers. On July 19, 2019 the company found the security breach which customers learned about officially on July 29, 2019. Affected Individuals approximately 106 million people in the U.S. and Canada.Personal details including name, address, credit score, account limitations, debts and credits, account history alongside contact information were stolen from Capital One in this breach. Moreover, 140,000 SSNs and 80,000 bank account connections became exposed (one, 2025).

2.2 Past Similar Breaches

Equifax Breach (2017) – Exposed personal data of 147 million individuals due to unpatched vulnerabilities.

Yahoo Data Breach (2013-2014) – 3 billion accounts compromised due to weak security controls.

How the Breach Happened

Firewall Misconfiguration: Capital One's cloud-based firewall had an incorrect configuration, allowing external users to query and access internal resources without proper authentication.

Unauthorized Access: Thompson exploited this misconfiguration using a specialized script to extract data.

Data Extraction: Over a period of months, data was gradually extracted from the compromised AWS S3 buckets.

Online Posting: Thompson stored stolen data on GitHub, which was later discovered by an ethical hacker.

Legal Consequences: Capital One was informed, and the FBI arrested Thompson shortly after.

2.3 Evolvement of the Breach

An attack on Capital One happened when the company accidentally left its web application firewall improperly set up on Amazon Web Services. As a former AWS employee Paige A. Thompson took advantage of her cloud server knowledge to expose and target the system vulnerability. She

made a scanning device to detect AWS security flaws which she used to steal data from more than 30 companies plus Capital One.

2.4 Intention Behind the Breach

Thompson wanted to earn status among hacking experts as her main driving force. Through her online profile as unpredictable she described her cyber exploits on GitHub and social networks without keeping them private. Research shows Thompson did this without trying to profit from the stolen information or distribute it for payment (Waldman, 2022).

2.5 Impacts of the Breach

The data breach created multiple major effects for the company.

Capital One needed to spend $150 million to $100 million for tasks related to customer communication, credit monitoring, IT expenses, and legal representation.

The Office of the Comptroller of the Currency fined Capital One $80 million due to inadequate risk analysis before moving essential IT services into the public cloud environment.

Capital One needed to increase cybersecurity after paying $190 million to settle guest lawsuits.

The incident broke customer confidence and showed customers Capital One did not fully secure their data when using cloud technology (one, 2025).

2.6 Statistical Overview

The Capital One data breach became one of the biggest cyber incidents ever recorded due to affecting 100 million people. Since 2017 Equifax reported 147 million victims while Yahoo disclosed three billion user accounts affected in their cyberattacks from 2013 to 2014. The recent breaches show how essential it is to develop powerful cybersecurity methods to safeguard customer private information.

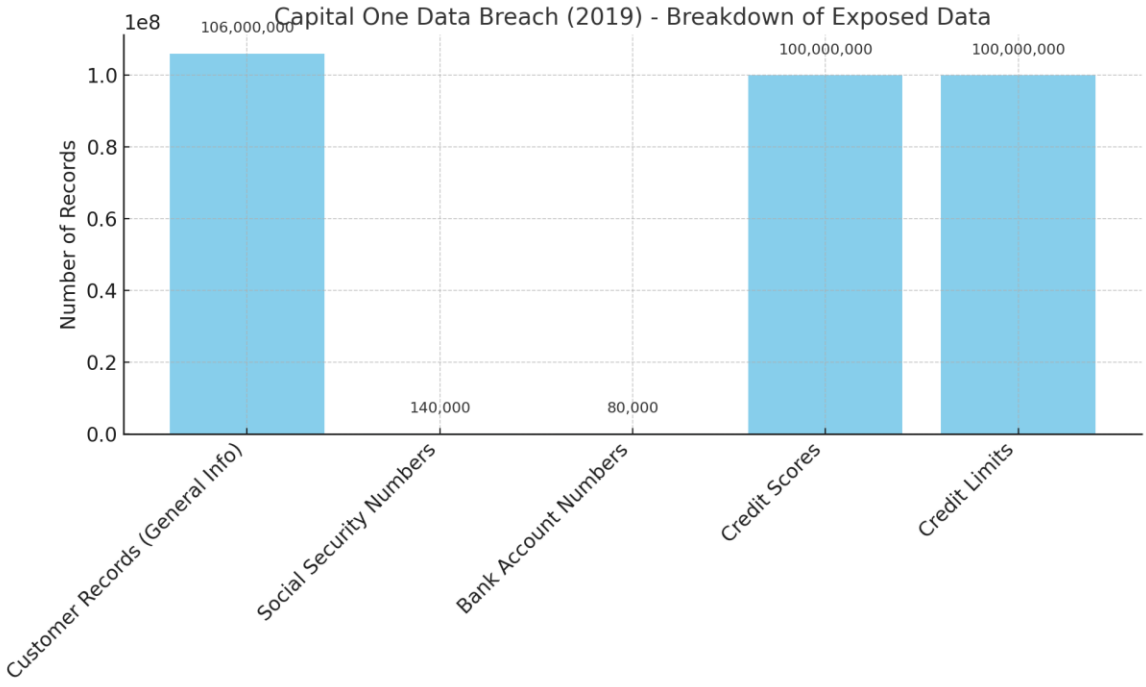


Figure 1-graphical representation

3. SOCIAL ISSUES

3.1. Background on Social Issues

The impacts of misused technology on both people and communities make up the social concerns of cybersecurity. The social impacts of data misuse extend far beyond money loss since they hurt both people's mental well-being and make society less trustworthy and equal.

3.2. In the Capital One breach:

1. Erosion of consumer trust:

Brutal data breaches destroy the trust of consumers in organizations that manage personal information. Organizations which suffer breaches experience significant customer trust erosion because most people abandon their business with these affected entities according to research findings. According to an industry research more than two thirds (65%) of consumers decrease their trust in organizations when data breaches occur which leads them to end business relations. or switch to alternative providers Capital One customers began doubting the bank's security capability after it became known that 106 million people received data exposure (Siddhant Mishra, 2024).

2. Emotional and psychological harm:

Data breaches create both emotional and psychological trauma which exceeds financial losses as they cause significant distress to affected individuals. The discovery that data thieves obtained your personal information can trigger intense traumatic reactions. Scientific studies show that victims of identity theft experience serious emotional traumas which cause them to feel humiliated and disappointed alongside frustration and stress and anxiety and at times lead to depression and damaged personal bonds soon after the attack (Marc Deliema, 2021).

3. Impact on vulnerable population:

Several factors concerning social status determine how severely data breaches affect different groups of people. Studies show older adults together with racial minorities and low-income members face much greater financial injuries and psychological trauma from identity theft incidents thus social inequalities worsened the damage of this data breach. These types of breaches

specifically affect vulnerable groups like credit card applicants who typically include students and retirees alongside low-income individuals. Therefore, the incident demands care and support for these population groups (Marc Deliema, 2021).

Cloud and Corporate Responsibility:

The incident led to society-wide discussions which analysed to what extent cloud providers and corporations should handle data security. Two prominent figures such as U.S. Senator Ron Wyden along with congressional bodies started analysing capital One and AWS cloud security practices after the breach. People asked themselves two critical questions in public: “Are cloud providers secure enough to protect our data?” and “Do banks need to depend on third-party platforms to such an extent?” The security incident strengthened doubts about how well firms maintain their security competencies while adopting cloud-based systems (ennis, 2023).

Reluctance to Share Personal Information:

Data breaches cause widespread unwillingness for people to disclose their personal data which constrains the growth of digital economies. Research demonstrates that data breaches make numerous consumers restrict their data sharing with companies across the following period. The Capital One incident probably encouraged customers to protect their privacy by becoming less trusting of online form requests. Society faces this concern because contemporary online platforms including banking portals and e-commerce interfaces and medical portals require customers to offer correct personal data for service access (Siddhant Mishra, 2024).

4. ETHICAL ISSUES

4.1. Background on Ethical Issues

The concept of ethical issues relates to correct and incorrect ways investigators deal with data while responding to security incidents and handling customer interactions. Security practices in cybersecurity meet ethical standards when organizations protect privacy while sharing transparent information and take duty to prevent breaches with appropriate purposes.

4.2. In the Capital One case

1.Duty to Protect Customer Data: As a data collector Capital One held responsibility for protecting all acquired personal information. In Kantian duty ethics the unethical handling of customer data represents a violation of how individuals deserve respect and the maintenance of promises. The bank previously represented to customers via an unexpressed promise that it would safeguard their information yet its systems failures compromised this guarantee. From a utilitarian standpoint the company is committing wrongdoings due to the massive damage it inflicted upon millions that exceeds any potential favorable repercussion from having weak security measures. From a utilitarian standpoint there is no wider beneficial outcome from reducing security standards (acm, 2018).

2.Individual Privacy vs. Data Collection: Many financial institutions routinely receive and preserve personal data including Social Security numbers which would become dangerous if released to unauthorized locations. Relatively speaking one needs to determine if maintaining and obtaining vulnerable personal data stands as a legitimate practice. The framework of Rights theory defines the right for people to maintain privacy about their information. Individuals who granted authorization for data collection may not have agreed to extensive usage or potential risks against their informational rights as described by rights theory. The security incident indicates Capital One collected personal data carelessly which results in ethical concerns about privacy protection across all relevant frameworks (acm, 2018).

3.Transparency and Honesty with Stakeholders: Capital One issued a formal apology after the breach while collaborating with law enforcement but its customers discovered full details by reading news reports. All companies maintain an ethical obligation to be honest with their clients. According to deontological ethics duty of truth requires people to unveil security flaws leading honesty to become a crucial principle. Capital One demonstrated responsibility through their

prompt public admissions which match this obligation. At the core of virtue ethics lie characteristics like honesty and accountability which enable the CEO's apology to be viewed as virtuous (acm, 2018).

4.Responsibility of the Hacker (Individual Ethics): The criminal action committed by the hacker Paige Thompson involved illegal data theft. The categorial imperative requires not willing any crime or data exploitation into universal laws thus making them immoral according to Kantian deontological principles. Through online bragging Thompson violated both the ethical principles of respect for property and privacy boundaries.

5.Role of Cloud Provider and Shared Responsibility: Some people argue that the fault lies with Capital One, while others will tell you that Capital One’s error was overshadowed by Amazon’s or AWS. One can do duty and rights on both sides in an ethical sense. It was deontologically argued that both sides had a duty to maintain security, Capital One had a duty to set up, monitor the system correctly, and AWS had a duty to provide secure cloud infrastructure.

5. Legal Issues

5.1 Background:

Failure to protect personal data by organizations leads to legal cybersecurity issues because it violates privacy laws and security regulations as well as contractual obligations. The Capital One breach resulted in enforcement actions alongside financial penalties together with class-action settlement costs because of violations under Computer Fraud and Abuse Act (CFAA) and Gramm–Leach–Bliley Act (GLBA) and multiple data protection legislation statutes.

5.2 In capital one

1.Criminal Prosecution (Computer Fraud and Abuse):

Hacked under U.S. federal law (Ex. 18 U.S.C. § 1030: Computer Fraud and Abuse Act, et al.). The Department of Justice's own complaint alleges computer fraud and abuse for unauthorized access to Capital one's stored data (justice, 2022). Paige Thompson was found guilty on several counts of wire fraud and unauthorized access to a protected computer in June 2022. This is an outstanding example of this issue, it demonstrates how serious the federal crimes of hacking and data theft really are and spell out the penalties that include imprisonment from the legal perspective, it speaks to the enforcement of cyber-crime laws and the process of investigating and prosecuting such breaches (ennis, 2023).

2.Privacy and Data Protection Laws:

As a bank, Capital One is bound to certain levels of data protection regulations. This includes Gramm–Leach–Bliley Act (GLBA) and its interagency guidelines on safeguarding customer information in the U.S. Under GLBA financial institutions must deploy security systems while they are obligated to tell their customers about data breaches. Included in the breach were several state data breach notification laws (requiring prompt explanation to affected individuals) and potentially federal laws such as the Fair Credit Reporting Act (for any information regarding credit). Furthermore, Canadian law prevailed, as the data affected 6 million of the 10 million Canadians governed by the Canadian law, namely Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Such incidents are banned by laws in both countries that allow regulators to sanction such things (hewardmills, 2019).

3.Regulatory Enforcement and Fines:

The United States financial authorities enacted specific penalties against Capital One. The Office of the Comptroller of the Currency imposed an $80 million civil penalty on Capital One during August 2020. The OCC imposed a penalty which stated Capital One had neglected to conduct proper risk assessments before shifting important IT operations to a public cloud solution and required the bank to create formal plans from board members. Capital One received approval from the Federal Reserve in 2023 to remove its security-deficiency consent order as the bank met acceptable standards of security (occ, 2020).

4.Civil Litigation and Class Actions:

The legal reaction to this data breach produced a customer class-action suit against the company. Customers filed suits that accused Capital One of negligence in addition to contract violations and consumer protection law breaches when the company neglected to protect personal data. Capital One resolved multiple customer privacy lawsuits through a $190 million class action settlement during the later period of 2021 (ennis, 2023). The resolution became finalized after the court approval. Under the terms of settlement Capital One agreed to compensate millions of consumers with credit monitoring services and additional expenses. The litigation analyses both the corporate legal responsibility for data breaches as consumers explore various legal procedures to seek compensation (hewardmills, 2019).

5.International and Cross-border Law:

The breach affected persons located in both the United States and Canada leading to legal questions concerning international regulations and inter-border agreements. Both Canadian authorities through the Office of the Privacy Commissioner as well as U.S. state attorneys from jurisdictions including Massachusetts and New York displayed their interest in the investigation. According to PIPEDA Capital One must notify both the regulator and all individuals whose Canadian data was exposed in a breach. The Washington Privacy Act together with other U.S. state laws have jurisdiction over data belonging to state residents. The incident brought attention to how U.S. cloud providers should adhere to data protection standards equivalent to the EU's GDPR when their data storage bases are predominantly located in the U.S. A legal issue stemmed from the various national laws which intersected during multi-jurisdictional data breaches when determining who has enforcement powers and what rights consumers possess. Standards and remedies must be understood differently based on international borders.

6. Professional Issues

6.1 Background

The incident needs examination from a professional perspective under ACM Code of Ethics and Professional Conduct to evaluate compliance with standards established for computing professionals.

6.2 In capital one

1.Ensuring Security and Avoiding Harm:

All professionals working in computing sectors must promise to safeguard others from harm. The cloud systems at Capital One were configured and monitored by the company staff together with their contractors. ACM Principle 1.2 (Avoid Harm) defines undesired informational disclosure cases as forms of professional mis-behaviour. Such risks should have been minimized by professionals yet at this point they became real. ACM terms show that their failure to prevent expected damage constitutes negligence. Under the Code there exists a requirement to report any system vulnerabilities that might result in harm to others. A professional issue emerges when those responsible do not complete their data security tasks and fail to report potential vulnerabilities according to the ACM Code requirement for harm prevention (acm, 2018).

2.Respect for Privacy:

Activists should employ personal information exclusively for legitimate purposes and prevent unauthorized access according to Principle 1.6 in the ACM Code (Respect Privacy). Capital One professionals acquired various personal records that required them to exercise caution about unauthorized data collection according to Code standards. The security breach demonstrates that necessary pre-cautionary measures did not work. ACM provides guidelines that professionals should maximize the utility of their database storage capacity by retaining only essential information. The professionals at the company should analyze if their data handling procedures complied with this requirement. The Code standards for data minimization and transparency and protection were violated due to this security breach (acm, 2018).

3.Competence and Quality of Work:

Both process quality and product quality must be of high standard according to ACM Professional Responsibility 2.1. The cloud infrastructure with firewall configuration serves as a final product

developed from Capital One's information technology work. The security breach reveals poor work quality because the system administrators possessed too much access power while the firewall configuration remained inadequate in its design and testing phase. Similarly, Principle 2.2 urges maintaining high standards of professional competence and ongoing skill development (acm, 2018).

4.Transparency and Honesty in Communication:

According to ACM Principle 1.3 regarding honesty professionals should disclose all system-related details including functionality and problems. The response process at Capital One included announcing public disclosures while computing professionals must provide accurate information to both management and stakeholders regarding security problems. All employees who submitted cloud setup doubts needed to express their concerns according to principle-requirements. The company took ethical actions by informing the public quickly and reporting everything publicly following the breach (acm, 2018).

5.Compliance with Laws and Policies:

Professionals need to know and respect all existing rules as per the ACM Code 2.3 which includes both laws and regulations. The incident demonstrates that organizations must adhere to security-related laws including GLBA and OCC guidelines as well as internal policies. The banking industry must follow standards which regulate its minimum cybersecurity requirements. The failure to maintain security rules compliance stands as a professional issue stemming from mismanagement of systems by responsible personnel. Staff members at Capital One needed to execute all essential legal standards and protocols (GLBA and PCI DSS along with NIST frameworks) since these requirements formed the basis of their ethical mandate. This incident demonstrates how disregarding professional responsibilities leads to negative results (acm, 2018).

7. Conclusion and Personal Reflection

A major breakdown in cybersecurity management merged with ethical violations and legal non-compliance was revealed through the Capital One data breach in 2019. A massive number of people suffered harm because sensitive information remained widely exposed due to corporate responsibility deficiencies. Social trust suffered major damage because regulators through their penalties stressed the necessity for organizations to improve their risk management practices. Lawmakers started to see that respecting privacy rights along with preventing foreseeable harm cannot be ignored from an ethical perspective. The breach demonstrates why cybersecurity requires ethical and professional commitment since it extends beyond technical matters especially at a time when electronic data and cloud services have become crucial.

Personal Reflection

1. Brainstorming Phase

The persons impacted by the breach at Capital One consist of customers, employees, stockholders, regulators and cloud service Provider Amazon Web Services (AWS). Severe risks and possible outcomes such as trust erosion, lawsuits, negative public perception, people feeling anxious, and weaknesses in cloud storage were present. Ethical and professional challenges were related to mishandling customer data, infringing upon people's privacy, and failing to maintain appropriate security measures. Alternatively, creating new cybersecurity policies, raising public consciousness, and implementing stricter regulations were among the advantages that ultimately resulted from how the situation was handled. Actions that can be taken in such situations are assessing the pros and cons of each option. Many managers have to weigh options such as releasing information about the incident, enhancing security measures, keeping all parties informed, providing compensation where possible, or waiting to present the details to reduce the impact on their reputation.

2. Analysis Phase

The decision-makers are responsible for safeguarding data, promoting openness, and fulfilling their legal and ethical duties. People affected should be kept informed, protected from misuses of their information and compensated for any injuries they suffer. Each decision should be considered according to its relative ethical importance. Disclosing information promptly and enhancing the security system help consumers trust the organization while withholding information to avoid alarm could violate ethical norms. Both principles 1.2 (Avoid Harm) and 1.3 (Be Honest and Trustworthy) are expressly cited in the ACM Code of Ethics (ACM-org, 2025). Ethics requires that information be shared promptly and redress offered. Openly speaking is regarded as appropriate; remaining silent or withholding the information longer is unacceptable. Acting in the most ethical manner involves minimizing harm, ensuring openness, and rebuilding trust over time while adhering to defining ethical and professional standards.

8. References

acm, 2018. *acm.* [Online]
Available at: https://www.acm.org/code-of-ethics#:~:text=In%20this%20document%2C%20,This%20list%20is%20not%20exhaustive
[Accessed 25 4 2025].

ACM-org, 2025. *acm-org.* [Online]
Available at: https://www.acm.org/code-of-ethics
[Accessed 10 05 2025].

dias, d., 2022. *buscompress.* [Online]
Available at: https://buscompress.com/uploads/3/4/9/8/34980536/riber_11-4_06_t22-044_71-90.pdf
[Accessed 8 4 2025].

ennis, D., 2023. *Cybersecuritydive.* [Online]
Available at: https://www.cybersecuritydive.com/news/fed-ends-capital-one-breach-action/686970/#:~:text=The%20incident%20spurred%20questions%20as,gaps%20falls%20on%20Capital%20One
[Accessed 27 04 2025].

hewardmills, 2019. *hewardmills.* [Online]
Available at: https://www.hewardmills.com/the-legal-fallout-of-the-capital-one-data-breach/#:~:text=In%20the%20Information%20Age%2C%20where,will%20protect%20the
[Accessed 25 4 2025].

justice, U. d. o., 2022. *Us attorney's office.* [Online]
Available at: https://www.justice.gov/usao-wdwa/united-states-v-paige-thompson#:~:text=the%20criminal%20complaint%2C%20Thompson%20posted,seized%20electronic%20storage%20devices%20containing
[Accessed 25 4 2025].

Khan, S., 2022. *Association for computing machinery.* [Online]
Available at: https://dl.acm.org/doi/10.1145/3546068
[Accessed 8 4 2025].

Marc Deliema, 2021. The Financial and Psychological Impact of Identity Theft Among Older Adults. *Innovation in Aging*, 5(4).

occ, 2020. *office of comptroller of the currency.* [Online] Available at: https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html#:~:text=The%20OCC%20took%20these%20actions,Interagency%20Guidelines
[Accessed 25 4 2025].

one, c., 2025. *capital one.* [Online] Available at: https://investor.capitalone.com/news-releases/news-release-details/capital-one-announces-data-security-incident?utm_
[Accessed 8 04 2025].

one, c., 2025. *capital one.* [Online] Available at: https://www.capitalone.com/digital/facts2019/
[Accessed 8 04 2025].

Siddhant Mishra, M. G. T., 2024. *IJCRT.org.* [Online] Available at: https://ijcrt.org/papers/IJCRT2407563.pdf#:~:text=study%20by%20Ponemon%20Institute%20,on%20customer%20loyalty%20and%20retention
[Accessed 28 april 2025].

Waldman, A., 2022. *tech target.* [Online] Available at: https://www.techtarget.com/searchsecurity/news/252521775/Paige-Thompson-found-guilty-in-2019-Capital-One-data-breach
[Accessed 8 4 2025].