LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

CS5071NI - Professional and Ethical Issues

100% Individual Coursework

2024-25 Autumn

Credit: 15 Semester Long Module

Student Name: TENJI SHERPA

London Met ID: 23048523

College ID: NP01NT4A230174

Assignment Due Date: Monday, May 19, 2025

Assignment Submission Date: Monday, May 19, 2025

Word Count: 3258

Submitted to: Mr. Avinav Neupane

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.

TENJI SHERPA2.docx

Islington College Nepal

Document Details

Submission ID
trn:oid:::3618:96631353

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

Download Date
May 19, 2025, 11:56 AM GMT+5:45

File Name
TENJI SHERPA2.docx

File Size
21.5 KB

17 Pages

3,219 Words

18,532 Characters

turnitin Page 2 of 10 - Integrity Overview Submission ID trn:oid:::3618:96631353

2% Overall Similarity

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

Match Groups

- 0 Not Cited or Quoted 2%
  Matches with neither in-text citation nor quotation marks
- 0 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

2% Internet sources
0% Publications
1% 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.

turnitin

Match Groups

Top Sources

Top Sources

1 Internet
manulawblog.com <1%

2 Submitted works
Virginia Community College System on 2023-10-04 <1%

3 Submitted works
Coventry University on 2021-06-08 <1%

4 Submitted works
Colorado State University, Global Campus on 2024-02-05 <1%

5 Internet
thehill.com <1%

6 Internet
www.investopedia.com <1%

Table of Contents

TABLE OF FIGURES

1. Introduction

1.1 Introduction to Company

Capital One is a technology driven financial company that is passionate about making banking easier and more human for its customers. Incorporating the notion that information and technology could shake banking system, it has been progressive under the **CEO's**, **Richard Fairbank's leadership**. Its contemporary **headquarters** in **McLean, Virginia**, enables engineers, designers and data scientists to collaborate to build intelligent, real time customer experience. (One, 2019)

Figure 1.Capital One (Connolly, 2019)

1.2 Introduction to cyber threats and risks

The variety of **cyber threats** against corporations specifically aimed at **financial institutions** such as **Capital One** includes numerous attack vectors that exploit different network weaknesses. This section analyses different attack types together with their practical consequences and their relationship toward the contemporary cloud-based environment.

1.2.1 Insider Threats:

Malicious activity by workers or contractors who have access to the system. A former AWS engineer stole Capital One data by abusing privileged information. (Justice, 2019)

1.2.2 Misconfigurations in the Cloud

Exposed data as a result of cloud platforms **incorrect security** configurations. **Unauthorized access** to **S3 buckets** was made possible via a **misconfigured AWS firewall**, which led to the Capital One breach. (Krebs, 2019)

1.2.3 Delayed Detection

The breach at Capital One required multiple months for **discovery** because the company did not have proper **incident response** and **detection** procedures in place. Breach detection delays increase both **financial damage** and overall expenditure for the organization. (IBM, 2020)

1.2.4 Third-Party Risks

Target breach started because of **security vulnerabilities** which gave unauthorized parties entry through **supplier credentials**. The breach at **Target occurred** because an **HVAC contractor** lost control of their account credentials. (Krebs, 2014)

1.3 Background

There were massive **data leaks** in other large companies before to the **Capital One** breach. For example: **Equifax (2017):** Hackers got access to sensitive information of 147 million people because of a missing software update (Federal Trade Commission (FTC), 2022). **In 2019, Facebook** disclosed how its user data exposed through security flaws on **Amazon Web Services** server systems (Coulter, 2019). These cases indicated how **big financial companies** could be susceptible to cyberattacks. Capital One migrated most of its data to AWS computer cloud. A firewall (that protects data) was improperly configured. This mistake left a loophole in their system security. (One, 2019)

In March 2019, Paige Thompson, **a former AWS employee** discovered that hole and exploited it by getting into Capital One's storing in the cloud. She exploited a technique by the name Server-Side Request Forgery (SSRF) that allows reading about **30 GB of customer data**. (Capital One, 2019) She illegally obtained information on **106 million people** with their names, addresses, credit scores and Social Security numbers. Rather than selling the data, she discussed the breach on the online forums. Capital One was informed

about the breach by a security researcher who found it and reported to **Capital One in July, 2019**. Capital One notified the **FBI**. (One, 2019)

Capital One reported that it would invest about **$100– 150 million** in solving the problem, credit monitoring, and improving its systems (One, 2019). In 2022, the **company paid out $190 million to a class-action lawsuit** (Lab, 2025). **U.S. regulators** also made Capital One strengthen its cybersecurity systems. **Paige Thompson**, who was a hacker, was arrested and eventually found **guilty of committing wire fraud** and **hacking–related crimes**. (United States Attorney's Office, 2019)

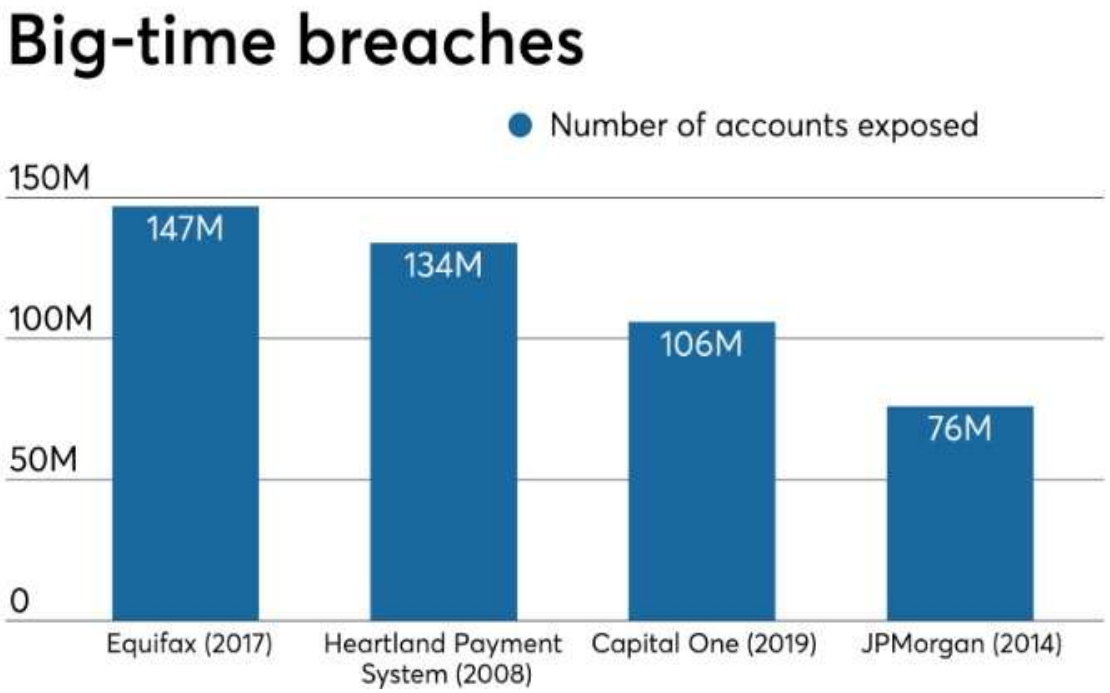

Figure 2.Capital one data breach (Crosman, 2019)

2 Social Issues

The social issue refers to a negative situation that disrupts personal and social aspects of community existence and societal groups and produces public confusion regarding its fundamental nature, root causes, and possible solutions. Social problem and social issue share similar meanings in modern society. (Britannica, 2024)

2.1 Privacy of Data and Personal Safety

The Capital One hack leakage revealed important **personal information**, including **Social Security numbers** and **bank details** of **106m people (in the United States 100m people, and in the Canada 6m).** This violation greatly raised the level of risk of identity theft and financial scams for users that were affected. The exposure of their private data in most cases exposed many victims to **emotional stress**. (Krebs, 2019)

2.2 Corporate social responsibility

Capital One failed to put in place appropriate **security controls** on its **cloud infrastructure** and it is this that was exploited by an ex-AWS employee to take advantage of **misconfigured firewall**. This lapse was a reflection of carelessness on the part of the corporate element to **protect customer data**. The incident enforced that corporations have the **ethical and legal duty** to protect employees from strong cyber security breach. (Griffith, 2019)

2.3 Need more strict control

The breach brought the **inadequacy** of current **federal data privacy laws** to the U. S. forefront again. The experts and lawmakers stress the need for more **stronger regulatory** control on companies that manage people's data. The event showed that the **lack of mandatory standards** means that a lot of organizations are failing to focus on **consumer data security**. (Knowledge, 2019)

2.4 Risks of Identity Theft

Hackers stole complete packages of information necessary to commit **identity fraud**, such as names, birthdates, address information, and financial records. These details enable inappropriate **financial transactions** and **fraudulent account creation**. The incident

highlighted how serious it was for the establishment of real time monitoring system and the pre-emptive measures to prevent such attacks. (Center, 2019)

2.5 Loss of Public Trust

After the breach occurred numerous customers **lost trust** in Capital One's capability to **protect their information**. The protracted time to **detect** and **report** the breach negative affected the company's **reputation**. Transparency and **quick response** are the requirement to **restore trust** of consumers following such cases. (Ducharme, 2019)

3 Ethical Issues

An ethical issue defines the situations that develop through moral conflicts needing resolution. People or organizations encounter such problems when right and wrong stand in opposition requiring them to make choices from available options grounded in their moral beliefs**.** (Dictionary, 2025)

3.1 Inability in Data Security: (Deontological)

Capital One made **configuration errors** in its **cloud firewall** which enabled hackers to retrieve **sensitive private client data** including **bank account information** and **Social Security numbers**. Capital One could have prevented the security weakness through proper implementation of established **security standards**.

An organization should carry out **moral** actions that serve the best interests of customers even when these actions might not yield direct outcomes. Capital One **breached its ethical responsibility** because they failed to **properly protect customer data**. (Newman, 2019)

3.2 Delays in Social Communication: (Rights)

The breach which happened in **March 2019** remained undetected until **July 2019** after which Capital One waited an additional **10 days** before telling customers about the incident which left consumers open to threats.

Everyone has the **right to know** when their **personal information is at risk.** Capital One committed a breach when it kept customers unaware of the exposure. (Congress, 2020)

3.3 Loss of Knowledge and informed permission: (Rights)

The company failed to explain to customers which **security measures** were used for data storage along with the potential data risks. The company showed insufficient **clarity** about their data processing systems.

The **principle of ethics** relies on the foundation of **complete knowledge** understanding. All users need to **receive information** regarding data usage terms in addition to understanding protection measures. The **breach of ethical standards** occurred when Capital One failed to provide proper consent to customers. (Knowledge, 2019)

3.4 Technology Ethics and Partner Responsibility: (Virtue Theory)

The capital one breach became possible because the **AWS cloud platform** contained **vulnerabilities**. The security responsibilities between Capital One and AWS existed yet Capital One neglected **proper assessment of third-party risks along with management responsibilities.**

Organizations must practice **ethical behavior** through **responsible** and dedicated **partnership** choices with **technology companies**. The **lack of integrity and responsibility** led Capital One to neglect its oversight duties. (Harwell, 2019)

3.5 Fairness, Parity, and Unfair Effects:(Rights)

The capital one security incident was caused by **inadequate security assessment** of their **AWS cloud services platform**. The leadership demonstrated poor oversight of technological management.

Organizations must demonstrate both **ethical behaviour** and **responsible conduct** for selecting strategic partners who handle **crucial data assets**. The **ethical principles of responsibility and integrity** were not maintained by Capital One. (Ducharme, 2019)

4 Legal Issues

A legal issue represents a query or situation that law administrators resolve through legal action. The nature of legal involvement may not be self-evident when unexpected illness creates employment uncertainties and demands clarification on mortgages and insurance. ((SRA), 2024)

4.1 Violation of Law: Gramm-Leach-Bliley Act (GLBA) of Federal Law

In 2019, access to over 100 million Capital One records was granted to unauthorized individuals because of a web application firewall issue in their cloud infrastructure. They had access to things like Social Security numbers, credit scores and the connection of accounts to credit cards. The hack was not noticed for quite a while, putting the customers at greater danger for identity theft and fraud.

By breaking the **GLBA rules**, the bank broke **a federal law** that requires financial companies to safeguard private data using good security practices. (Commission, 2025)

4.2 Negligence: Failure of Duty of Care under Common Law

Capital One was required to handle data security correctly to protect its customers. It failed to put in place sufficient protection or to monitor its systems closely. This is the reason hackers were successful in accessing the systems.

Neglecting their duty of care, **under common law**, since it is expected that companies take action to keep people safe. When Capital One did not meet this requirement, they failed legally to ensure data was secure. (Black, 2024)

4.3 Settlement: $190 Million Capital One Data Breach Class-Action Settlement

People were anxious and angry that their data had been stolen. Because of this, Capital One had to provide $190 million as part of a combined settlement to people who faced this issue.

While the company continued to declare it acted properly, the payment of $190 million settled the **rights in civil law** for harm caused by the data leak. People received payments

for their troubles, yet the settlement also pointed out that the company did not safely handle customers data. (Litigation, 2023)

4.4 Regulatory Fine: $80 Million Fine from the Office of the Comptroller of the Currency under Banking Regulation Law

The **Office of the Comptroller of the Currency (OCC)**, a US government agency, noted that Capital One did not follow the proper procedures when moving data to cloud storage. As the issue of known problems wasn't solved, the data breach was more easily carried out.

As a result, the company had to pay an $80 million fine **under the rules of federal banking law** for failing to protect customer data properly. Clearly, if a company does not manage risks and plan properly, major penalties can be imposed by regulators. (Currency, 2020)

4.5 Criminal Act: Violation of the Computer Fraud and Abuse Act (CFAA)

A former employee of Amazon Web Services named Paige Thompson entered Capital One's systems using a known bug and took a large amount of private customer information. Her illegal access demonstrated that Capital One's security in the cloud was not strong enough.

The actions broke the **Computer Fraud and Abuse Act (CFAA), a federal law** that makes it illegal to gain access to computer systems without permission. Hackers are stopped by the law and punished for stealing private information. (Department of Justice, 2019).

5 Professional Issues

5.1 Introduction to profession and Professionals

A profession is formed by specialists who study and train in a recognized field and use their knowledge and skills to serve the public (Australia, 2023). Professional issues represent work-related ethical matters and legal matters and practical challenges which influence both conduct and decision-making and professional standard adherence in workplace settings. Professional issues in the workplace involve four categories that include conflicts of interest and confidentiality violations and workplace ethics and regulatory compliance and professional accountability requirements.

5.1.1 Negligence in Security Configuration

The Capital One breach was primarily caused by poor security practices and misconfiguration of AWS cloud infrastructure through a firewall that failed to protect the system. A lack of system audits along with security testing proves essential for maintaining good cybersecurity practices. Capital One suffered a major breach due to its lack of implementation of accepted industry best practices. (One, 2019)

The **ACM Code of Ethics** directs computing professionals to design protected robust systems that resist security failures. Those working in computing should assure that systems are secure and avoid inflicting harm on anyone. ((ACM), 2018).

5.1.2 Breach of Privacy and Trust

Every customer's sensitive personal detail with Social Security Numbers and addresses and credit scores became accessible in the breach. The breach of privacy and erosion of customer trust. The unethical behaviour of Capital One caused substantial legal penalties and a major damage to their reputation. (Protess, 2019)

The **BCS Code of Conduct** establishes that both individual freedom rights and personal data protection have to be respected. All members should be mindful of privacy and keep information confidential. (BCS, 2024).

5.1.3 Lack of Cloud Security Expertise

Capital One's security problems came from a shortage of staff who specialized in cloud security at the time of the breach. Companies that follow AWS cloud services need to modify their security approaches along with their configurations and respond to novel threats. A lack of complete cloud safety protocol understanding by Capital One security professionals led to crucial mistakes in security configurations. (One, 2019)

According to the **Software Engineering Code of Ethics** engineers must limit their work to activities for which they possess acceptable training and qualifications. A person should only use technology on behalf of others if they have the needed skills or disclose any important limitations. (Society, 1999).

5.1.4 Failure in Communication and Information of Breach

The Capital One breach created a significant professional issue because public information about the breach showed up late while communication remained insufficient. Public disclosure of the Capital One breach started only in July 2019 after the March 2019 discovery. The delayed notification prevented affected customers from evaluating their dangers which led to an inability to take protective measures immediately. (Protess, 2019) The **Software Engineering Code of Ethics** requires engineers to quickly reveal and accurately disclose system malfunction threats that risk the safety of the public. Honesty and loyalty are required from engineers, so they should never say something that is not true or misleading. (Society, 1999).

5.1.5 Awareness and Control of Insider Threats

The incident revealed that AWS should strengthen its internal threat management systems because their attacker gained access through previous employee connection. The capital one internal security systems lacked proper capabilities to detect insider threats thus allowing the attacker to exploit system weaknesses privately.

According to the **ACM Code of Ethics** organizations should establish systems that both monitor and safeguard against employees who use internal knowledge to commit malicious acts. To prevent and manage threats from security breaches or ethical issues, organizations and professionals should set up appropriate processes. ((ACM), 2018)

6 Conclusion and Personal Reflection

6.1 Conclusion

The 2019 Capital One data breach proves that many things, from poor tech settings, lack of ethics, rule violations, and unprofessional actions by individuals, can come together to cause a significant cybersecurity incident. The incident revealed that over 100 million people had their personal and financial data stolen, making clear that security and threat control are still big challenges for most organizations.

As a result of the social breach, many became exposed to risks of identity theft and lost public trust. It was unethical for Capital One not to take proper care of customer information and delay telling impacted users. The company was accused of following the guidelines and was forced to cover monetary fines, settle lawsuits, and absorb charges from different regulators. There were several problems: inadequate supervision, missing knowledge about cloud security, and a lack of compliance with appropriate rules.

The report indicates that being proactive and responsible about cybersecurity is essential. All organizations are required to have effective security, inform stakeholders about what is happening, and follow the rules and laws. Advances in technology mean more attention is needed by companies to safeguard user details and build public confidence.

6.2 Personal Reflection

6.2.1 Brainstorming Phase

Stakeholders identified: The stakeholders are customers of Capital One, company employees, AWS partners, regulatory bodies, and the general public.

Risks: The dangers were someone unauthorized seeing private data, theft of identities, financial scams, and harm to Capital One’s reputation.

Consequences: The data breach brought about stress for users, consequences for the company, doubt among the public, and major compensation awards.

Benefits: After the attack, stronger safety measures were adopted. Individuals were given the option of having their credit report checked for free. The company improved after making the mistake.

Ethical/moral problems: Missing proper customer data protection, failing to reveal issues in time, and poor configuration practices raised issues about ethics.

Possible courses of action: Capital One could have used better security controls in the cloud, set up more effective monitoring, and told the public about the incident sooner. (Krebs, 2019)

6.2.2 Analysis Phase

Responsibilities of the Decision Makers:

- Capital One was required to ensure customer data remained secure.
- It was necessary for them to install the cloud system properly and check it on a regular basis.
- They had to train others and monitor possible events or risks from third parties such as AWS.
- The company should have informed everyone about the breach as soon as they found out.

Rights of Stakeholders:

- Both privacy and the protection of data were rights of the customers.
- They should have been informed if their data had been stolen.
- Regulators and partners should be able to share information truthfully and openly.

Impact of Actions and Consequences:

- Customer issues included concerns about their ID being stolen, increased stress and losing money.
- Capital One faced suits from customers, had to pay fines and lost the confidence of the public.
- The failure of the system was partly blamed on AWS's role.
- The delays that occurred worsened the situation and damaged more places.

ACM Code of Ethics (2018):

- Always be honest and trustworthy in your actions.

- Stay safe and also protect others' privacy. ((ACM), 2018)

Software Engineering Code of Ethics (1999):

- Put the interests of the public first.
- Make sure to represent any risks within the system in a straightforward manner.
- Don't handle jobs unless you're prepared. (Society, 1999)

Categories of Actions:

- **Ethically Obligatory:**

  Letting users know as soon as the breach is discovered, correcting misconfigurations, increasing spending on security and following established standards.

- **Ethically Prohibited:**

  Not revealing information, pretending some risks do not exist and not addressing security problems even after being cautioned.

- **Ethically Acceptable:**

  Together with AWS, updating training for employees and providing compensation to affected customers.

6.2.3 Recommendations

To prevent such issues in the future, **Capital One** needs to update its **cloud security** by frequently reviewing and adjusting their **firewalls** and **access systems**. You should regularly perform security checks, test for vulnerabilities and partner closely with **AWS** to make sure everyone understands who is responsible for what. Besides, workers must be updated regularly on cybersecurity to identify dangers, deal with data carefully and act properly in case of **incidents**. Companies must have a reliable team of cloud security experts to maintain their systems and comply with set guidelines in the industry.

A **timely** and well-communicated **data breach notification** should be a priority for Capital One. If someone's **personal data** is being put at risk, users must be informed promptly so they can protect themselves. The company must ensure they apply the **ACM and Software Engineering Codes of Ethics** to always be honest, remain accountable and respect **users' privacy.**

7 References

(ACM), A. f. C. M., 2018. *ACM Code of Ethics and Professional Conduct.* [Online] Available at: https://www.acm.org/code-of-ethics [Accessed 20 April 2025].

(SRA), S. R. A., 2024 . *Legal Issue – Choosing the right legal help.* [Online] Available at: https://www.sra.org.uk/consumers/choosing/legal-issue/ [Accessed 15 April 2025].

Australia, P., 2023. *What is a Professional?.* [Online] Available at: https://professions.org.au/what-is-a-professional/ [Accessed 20 April 2025].

BCS, T. C. I. f. I., 2024. *BCS Code of Conduct.* [Online] Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct [Accessed 22 April 2025].

Black, W. R. V., 2024 . *Questions About Tort and Contract Claims in the Cybersecurity Context Left Unsettled.* [Online] Available at: https://www.woodsrogers.com/insights/publications/questions-about-tort-and-contract-claims-in-the-cybersecurity-context-left-unsettled [Accessed 25 April 2025].

Britannica, E., 2024. *Encyclopaedia Britannica.* [Online] Available at: https://www.britannica.com/topic/social-issue [Accessed 5 April 2024].

Capital One, 2019. *Information about the Capital One Data Breach of 2019.* [Online] Available at: https://medium.com/nerd-for-tech/capital-one-data-breach-2019-f85a259eaa60 [Accessed 25 April 2025].

Center, N. C. L., 2019. *Statement Regarding Capital One Data Breach.* [Online] Available at: https://www.nclc.org/statement-regarding-capital-one-data-breach/ [Accessed 5 April 2025].

Commission, F. T., 2025. *Gramm-Leach-Bliley Act.* [Online] Available at: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act [Accessed 26 May 2025].

Congress, U., 2020. *Coronavirus Aid, Relief, and Economic Security Act (CARES Act),* Washington, D.C.: U.S. Government Publishing Office.

Connolly, J., 2019. *Capital One reveals huge data breach by hacker.* [Online] Available at: https://www.fintechfutures.com/data-privacy-security/capital-one-reveals-huge-data-breach-by-hacker [Accessed 22 April 2025].

Corporation, C. O. F., 2019. *Facts About the 2019 Cybersecurity Incident,* McLean, VA: Capital One.

Coulter, M., 2019. 540 million Facebook users' data was exposed on public Amazon servers. 3 April , pp. 12-15.

Crosman, P., 2019. *American Banker*. [Online] Available at: https://www.americanbanker.com/news/capital-ones-data-breach-was-bad-it-couldve-been-worse
[Accessed 05 April 2025].

Currency, O. o. t. C. o. t., 2020. *CC reports third quarter 2020 bank trading revenue.* [Online] Available at: https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html [Accessed 25 April 2025].

Currency, O. o. t. C. o. t., 2020. *In the Matter of Capital One, N.A. (Enforcement Action #2020-089)*, Washington, DC: U.S. Department of the Treasury.

Dictionary, B. L., 2025. *Ethical Issue.* [Online] Available at: https://thelawdictionary.org/ethical-issue/ [Accessed 6 April 2025].

Ducharme, J., 2019. The Capital One Data Breach Compromised 100 Million People's Data — Here's What to Do Now. *TIme*, 30 July.

Federal Trade Commission (FTC), 2022. *Equifax Data Breach Settlement.* [Online] Available at: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement [Accessed 23 July 2025].

Fung, B., 2023. *Capital One data breach: What you need to know*, s.l.: CNN.

Griffith, E., 2019. *Capital One Data Breach Compromises Data of Over 100 Million.* [Online] Available at: https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
[Accessed 5 April 2025].

Harwell, D., 2019. *Capital One looked for cloud security. Its own firewall couldn't stop the hacker.*. [Online] Available at: https://www.washingtonpost.com/technology/2019/07/30/capital-one-looked-cloud-security-its-own-firewall-couldnt-stop-hacker/
[Accessed 5 April 2025].

IBM, 2020 . *Cost of a Data Breach Report*, Armonk: IBM Security.

Justice, U. D. o., 2019. *Former Amazon Technical Employee Charged With Hacking Capital One*, Seattle, WA: U.S. Department of Justice, Western District of Washington.

Justice, U. D. o., 2019. *Tech Worker Arrested for Data Theft Involving Large Financial Services Company*, Washington, D.C.: U.S. Department of Justice.

Knowledge, P., 2019. *Capital One Data Breach Reinforces Need for Strong Consumer Privacy Protections.* [Online] Available at: https://publicknowledge.org/capital-one-data-breach-reinforces-need-for-strong-consumer-privacy-protections/
[Accessed 5 April 2025].

Knowledge, P., 2019. *Capital One Data Breach Reinforces Need for Strong Consumer Privacy Protections.* [Online]
Available at: https://publicknowledge.org/capital-one-data-breach-reinforces-need-for-strong-consumer-privacy-protections/
[Accessed 6 April 2025].

Krebs, B., 2014. *target Missed Alarms In Epic Hack of Credit Card Data,* New York: Forbes.

Krebs, B., 2019. *Capital One Data Theft Impacts 106M People,* s.l.: KrebsOnSecurity.

Krebs, B., 2019. *What We Can Learn from the Capital One Hack.* [Online]
Available at: https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/
[Accessed 3 April 2025].

Lab, H. F., 2025. *Capital One Data Breach Settlement: Payout Amounts, Eligibility Details, and Payment Timelines.* [Online]
Available at: https://hunterflylab.com/capital-one-data-breach-settlement-payout-amounts-eligibility-details-and-payment-timelines/
[Accessed 20 April 2025].

Litigation, I. r. C. O. I. C. D. S. B., 2023. *In re: Capital One Inc. Customer Data Security Breach Litigation.* [Online]
Available at: https://www.capitalonesettlement.com/Content/Documents/Notice.pdf
[Accessed 25 April 2025].

Newman, L., 2019. The Capital One Hack Hit More Than 100 Million People. *WIRED,* 29 July .

Newman, L. H., 2019. *Everything We Know About the Capital One Hacking Case So Far.* [Online]
Available at: https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/
[Accessed 5 April 2025].

News, C., 2018. *Facebook loses $119 billion in Wall Street record,* Los Angeles: CBS News.

Office, U. G. A., 2018. *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* Washington, D.C.: U.S. Government Accountability Office.

One, C., 2019. *Capital One Announces Data Security Incident.* [Online]
Available at: https://www.capitalone.com/digital/facts2019/
[Accessed 5 April 2025].

One, C., 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 15 April 2025].

Perlroth, N., 2016 . Yahoo Says 1 Billion User Accounts Were Hacked. 14 December .

Protess, B. a. C. S., 2019. *Capital One Data Breach Compromises Data of Over 100 Million.* [Online]
Available at: https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
[Accessed 23 April 2025].

Society, A. f. C. M. a. I. C., 1999. *Software Engineering Code of Ethics and Professional Practice.* [Online]
Available at: https://ethics.acm.org/code-of-ethics/software-engineering-code/
[Accessed 22 April 2025].

The New York Times Company, 2014. *JPMorgan Discovers Further Cyber Security Issues.* [Online]
Available at: https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/
[Accessed 24 July 2025].

United States Attorney's Office, W. D. o. W., 2019. *United States v. Paige Thompson.* [Online]
Available at: https://www.justice.gov/usao-wdwa/united-states-v-paige-thompson
[Accessed 25 April 2025].