

**LEVERAGING MACHINE LEARNING ALGORITHMS to LOWER FRAUDULENT
ACTIVITIES**

by

Student name

DB-FPX8840

Professor Name

Submission Date

_____, PhD, Dean

School of Business, Technology, and Healthcare Administration

A Capstone Work Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Business Administration

Capella University

Month & year of dean's approval

Commented [Dr. T1]: Maja Zelihic, PhD, Dean
School of Business, Technology, and Healthcare Administration

© Learner name, year

Abstract

The intent of the abstract is to give an overview of important aspects of your capstone project in a brief and concise manner. Use a single block style paragraph for the abstract, and have no indent. Write on the following topics (not more than 400 words). Research topic summary (1-5 sentences), a short summary of your capstone research topic. Justify your study and why the study the capstone needs is necessary. Write Research Questions, as written in your capstone parts. Research Methodology (1-2 sentences). Give a brief overview of the research methodology for the study. Population (1-2 sentences) and sample (1-2 sentences). Define the population and sample as well as high-level information about the sample's demographic characteristics. If the data were collected from a secondary source, describe the data collected. Data analysis (1-2 sentences): Give a brief overview of your data analysis. Findings (1-3 sentences): Give a brief summary of the findings and conclusion(s) of your research. Explain what the implications of your project are in practice and the deliverable that you produced.

Tips for Developing a Quality Abstract. (a) The abstract is representative of your work.

The abstract is not always read by most of the researchers if the paper is not relevant to their literature review or is not worth reading. The proposed abstract will be read (or previewed) by people in your discipline to gain insight into what kind of doctoral research you are doing and how well you are doing it. In this way, the abstract is a document of your PhD work. (b) Other instructions for creating an abstract are in section 3.3 of the American Psychological Association Publication Manual (7th edition) or on Campus at Academic Writer.

[https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-](https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-59?group=All&view=list&term=abstract&sort=asc)

[59?group=All&view=list&term=abstract&sort=asc](https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-59?group=All&view=list&term=abstract&sort=asc) (c) References are generally not used in the abstract, as the focus is the study, the research, and the findings.

Formatting for the Abstract. Write the abstract in block style (no indentations on the first line) that is double spaced. Move the text to the left, flush left and ragged right. Don't justify the right-hand margin. Avoid using headings, bullets, or bold. The Abstract page is not numbered, and “Abstract” does not appear in the Table of Contents.

ONCE YOU’VE WRITTEN THE ABSTRACT PAGE, DELETE ALL
INSTRUCTIONS.

Dedication

This dedication page is a voluntary (optional) service. It's your recognition of their value and esteem of those that have been important in your life. The dedication is personal; therefore, it's very common to have people included by their name that have no connection to the capstone topic.

One or two people are usually responsible for giving them the value and motivation to achieve excellence in the learning process, commonly known as the "payback" to those who taught them. Capstones can be dedicated to people who are important in learners' lives, often to family members, close family members, or to someone of importance to them.

Do not mention any names, or any names associated with the research site. Individuals can be mentioned by their title (e.g., the research director and the site proctor) but without their name (e.g., "Thanks to the research director and site proctor for their help"). Or you can mention people, but not link them to the site (e.g., "Thanks to the help of Abdul Ibrahim and Mary Carson"). In general, don't include the name of the site.

Note: if the Abstract runs onto a second page, change the page number of the Dedication to 4.

ONCE YOU'VE WRITTEN THIS PAGE, DELETE ALL INSTRUCTIONS.

Acknowledgments

This page of acknowledgments is a voluntary page. Acknowledging others – the acknowledgments are to people who have aided you in your research for the advanced doctoral manuscript or who have had a role in your scholarly career that is related to your research on the advanced doctoral manuscript. This could include a mentor, committee members, advisor(s), online/colloquia faculty, and other support persons from Capella or other organizations. List any fellowships, grants, or other organizational supports received in this section. The acknowledgments can also be used to thank statisticians, transcriptionists, etc., or to get permission to use an instrument.

Do not mention any names, or any names associated with the research site. Individuals can be mentioned by their title (e.g., the research director and the site proctor) but without their name (e.g., “Thanks to the research director and site proctor for their help”). Usually, don't mention the name of the site, but do name the people without association to the site (e.g., “Thanks to Abdul Ibrahim and Mary Carson for their help”). Permission to use an instrument is often one of the reasons for thanks by the learners.

ONCE YOU’VE WRITTEN THIS PAGE, DELETE ALL INSTRUCTIONS.

Table of Contents

Acknowledgments.....	4
List of Tables	7
List of Figures	8
SECTION 1. PROJECT DESCRIPTION.....	9
Overview of the Project	9
Problem Statement and Purpose	11
Theoretical Framework	14
Project Context.....	19
Historical Background and Current Trends	19
Synthesis of the Scholarly Literature	19
Synthesis of the Practitioner Literature.....	19
Alignment of the Project With the Literature and Discipline	20
SECTION 2. PROCESS	21
Project Questions	21
Project Design/Method	21
Stakeholders, Participants, and Target Audience	21
Role of the Researcher	21
Project Study Protocol	21
Sample.....	21
Data Collection	21
Ethical Considerations	21
Data Analysis	21

SECTION 3. FINDINGS AND APPLICATION	23
Relevant Outcomes and Findings	23
Application and Benefits.....	23
Implications.....	23
Recommendations for Policy	23
Recommendations for Practice	23
Recommendations for Future Work.....	23
Conclusion	23
REFERENCES	24
APPENDIX A. TITLE OF APPENDIX A	27
APPENDIX B. TITLE OF APPENDIX B	28

ONCE YOU’VE WRITTEN THE TOC, DELETE ALL INSTRUCTIONS.

List of Tables

Table 1. Set Table and Figure Titles in Title CaseXX

Table 2. TitleXX

ONCE YOUR LIST IS COMPLETED, REMOVE INSTRUCTIONS
AND UPDATE THE PAGE NUMBERS.

DELETE THIS PAGE IF NOT NEEDED.

List of Figures

Figure 1. Set Table and Figure Titles in Title CaseXX

Figure 2. TitleXX

ONCE YOUR LIST IS COMPLETED, REMOVE INSTRUCTIONS
AND UPDATE THE PAGE NUMBERS.

DELETE THIS PAGE IF NOT NEEDED.

SECTION 1. PROJECT DESCRIPTION

Overview of the Project

While the digital age has brought an age of convenience and ease to financial transactions perhaps never seen before, it has also brought a greater magnitude to the overall issue of financial fraud within the United States. The financial industry is constantly battling increasingly sophisticated fraud attacks, ranging from schemes that involve credit card fraud, identity theft, wire transfer fraud, and account takeover attacks (Afjal et al., 2023). Additionally, in the third quarter of 2024, credit card fraud reported by American consumers totaled about \$58 million, the lowest of the year (Statista, 2025). The number underscores the urgent need for smart and responsive systems for fraud detection that work in real-time to detect and prevent illegal activities.

Traditional fraud detection strategies rely on humans, are rule-based, and may not be able to respond to the new fraud challenges in financial institutions. The introduction of new technologies such as artificial intelligence (AI) and machine learning (ML) algorithms opens up opportunities for more sophisticated and agile approaches to fraud detection via algorithms (Pattnaik et al., 2024). Completely using AI technologies for fraud detection is not something that some financial institutions are doing (CIO, 2024). More than just technology is needed; organizational managers need to think in terms of a Management-Driven Approach to Innovation (McKinsey & Company, 2022) to devise fraud schemes. Limited use of fraud detection tools can be traced back to resistance to change, lack of leadership, uncertain organization, and poor cross-functional integrity. The difficulties underscore a need for practice advancement, specifically around the need for many general managers to have a clear plan on how to incorporate AI strategic and operational frameworks at institutions.

With the surge of digital transaction volume and speed, the financial sector in the U.S., especially banks and financial technology (fintech) companies, faces a heightened risk of fraud (Brogi & Lagasio, 2024). As advantageous as real-time payment systems may be, they provide few chances for manual fraud intervention (Vanini et al., 2023). The pressure is high on institutions needing to have the right fraud detection system to detect anomalies, red flag suspicious activity, and automatically take corrective action in milliseconds. According to Abikoye et al. (2024), a strong link between ML capabilities and organizational goals significantly curtails fraud committed in financial institutions. Bevilacqua et al. (2025) emphasized the importance of managerial skills and organizational readiness for realizing the value of the business through ML initiatives. The organizational activities are key to the ultimate success of fraud detection efforts and risk exposure.

The project goal will be to use the ML algorithms to reduce fraudulent activity in financial institutions in the U.S. The ML-driven anomaly detection capabilities can serve as a powerful tool for managers to implement an effective fraud prevention system, preventing fraudulent activities. The ability to detect anomalies through ML can be a valuable asset for managing an effective fraud prevention system to thwart fraudulent activities (Dama et al., 2024). According to Gupta et al. (2025), the main issue identified is a lack of leadership strategies to implement the ML technology to combat fraud activities in financial institutions. What is the problem being solved? The management in financial institutions usually does not have the strategic thinking and working mechanisms necessary to adopt advanced technologies like ML to respond to financial fraud, Chenguel (2020) reports. When technologies exist, the gap is in practice because of the lack of managerial ability to embed technologies in practice and decision-making. The project is important in that it will deliver decidedly important value to financial

organizations and will help to create a more secure financial system for consumers, as it aims to actively identify and impede any fraudulent transactions.

The impact of this project could give financial institutions' managers new insights on preventing financial losses by detecting fraud quickly and accurately. By effectively using the leadership methods, it can support implementing ML technology and mitigating fraud events by anticipating fraud (Bevilacqua et al., 2025). Therefore, a culture of innovation by leveraging ML could assist with combating the new challenges in fraud and improve the financial position of the organisation. Hence, the project is guided towards solving a problem in the general management of a business, which in this case is the inefficiency of the deployment and administration of the Smart Fraud Detection System. This project's data, which highlights the importance of considering managerial elements of ML implementation for fraud prevention, could represent a pathway for financial institutions aiming to modernize their efforts and ensure security and trust in the digital landscape.

Problem Statement and Purpose

When fraud occurs, there is a general business problem: loss of business profitability and decline in customer satisfaction (Feingold & Wood, 2024). Organizations are not equipped to detect fraud and are hit with the impact of fraud by their traditional fraud detection systems. The Federal Trade Commission (FTC) estimates that Americans lost \$90 - \$501 million due to fraudulent activities (FTC, 2025). As the losses continue to increase, it becomes clear that fraud is not only a constant threat but also is becoming more sophisticated, posing a significant threat to both the consumer's trust and the organization's stability.

The business problem is that some technology managers in the U.S. financial industry (Lamey et al., 2024) have not had effective resources and technology strategies to implement ML

fraud protection. However, financial institutions have access to the technologies, but there are lots of instances where, due to the incompetence of their leadership and lack of strategic support, the implementation of those fraud detection technologies fails, impacting the organization's performance (Afjal et al., 2023). One key factor cited is the lack of leadership in integrating high-tech solutions, leading to alleged fraud by customers who report about 2.6 million cases (FTC, 2025). This specific business problem leads to various consequences such as ongoing exposure to fraud risk, loss of customer trust, and huge financial losses (Lamey et al., 2024). The association of technology competence and strategic management is one of the crucial aspects in the overall problem of general management in financial institutions.

Alignment with Program

The project on leveraging ML technology is perfectly aligned with the Doctor of Business Administration (DBA) program, with the project tackling a high-impact business problem in the finance industry, in the role of strategic leadership within the financial institution. Financial fraud is another of the most expensive and complicated problems faced by the banking and financial services industry (Hilal et al., 2021). Accordingly, the project aims to examine the role of strategic mismanagement in the lack of successful ML adoption resulting in financial losses, regulatory risks, and reputational harm. The issue highlighted the significance of the role the leadership could play to enhance financial functioning through the incorporation of ML technology (Pattnaik et al., 2024). The work of this project, therefore, is a perfect fit for the Doctor of Business Administration (DBA) concentration in interdisciplinary leadership and strategic management. Analyzing the financial manager's ability to make the decision to adopt advanced technology also offers a helpful perspective on how to better align the organization with advanced technology on the fiscal side and reduce the likelihood of fraud (Dama et al.,

2024). The intake for the project under the DBA is to address complex problems in the industry that can be resolved by applied research.

Purpose Statement

This generic qualitative inquiry project aims to find out the technology manager's point of view in the USA financial industry who implemented resources and technology strategy to implement ML fraud detection and protection. The project will delve into ideas of leadership approach in the adoption of ML technology for fraud detection (Dama et al., 2024). The target population will be financial managers for the institutions in the banking and financial services industry in the United States.

Gap in Practice

The difference in practice is that some U.S. financial managers have not adopted proper fraud detection reducing strategies in their financial operations (Chenguel, 2020). The use of standard fraud detection systems is out of sync with fraudster techniques and is fraught with producing fraud. The gap in practice is not because fraud detection technologies are not available, but as a result of the absence of a leadership strategic approach towards implementing the ML technology (Hariyani et al., 2024). That gap means a specific problem: that financial institutions can face complicated fraud schemes that are able to circumvent detection by the current systems, with a monetary cost. The ideal state is to have managers of financial institutions actively leveraging ML to get predictive capabilities on fraud detection and prevention in real time with high precision (Pattnaik et al., 2024). Practitioner use of project findings may be valuable to those practitioners who wish to bridge the gap and highlight the value of adopting more advanced analytical approaches for the prevention of fraud. Also, they need to be analysed in the light of a company's overall strategic direction.

Theoretical Framework

The aim of the research is to learn about the perspectives of U.S. financial industry technology managers who have adopted resources and technology strategies to implement fraud detection and protection through ML. The theoretical model used as the basis of the qualitative study is the Technology Acceptance Model (TAM), which was developed in 1989 by Fred Davis (Davis, 1989). The TAM has been demonstrated as being explanatory to understand users' acceptance of emerging technologies and as a solid framework to explore the strategic, behavioral, and managerial aspects of the adoption of ML systems in financial institutions (FI) (Davis and Granić, 2024). The TAM has five main constructs, which are: perceived usefulness (PU), perceived ease of use (PEOU), attitude toward use, behavioral intention to use, and actual system use (Thatsarani & Jianguo, 2022). For the project, perceived usefulness is defined as the extent to which financial managers believe the financial managers will be more efficient in the organization with the use of an ML-based fraud detection system; it will improve the decision-making process in the organization and reduce the losses that can be caused by fraud.

PU is very closely related to the performance and strategic value the technology will be able to deliver on a business management level. Representing perceived ease of use (PEU), this level of belief suggests how easy managers and employees perceive installing and using ML systems to be for financial organizations (Joseph & Eaw, 2023). High PEOU increases confidence of use—and this is particularly true for those who might not want to engage in change due to the implementation costs. The other factors— attitude to use, intent to use behavior, and use of the system—show each step in the process of how attitude towards the technology can lead to intent to use behavior and then to use of the technology in action by managers.

Commented [Dr. T2]: Start out by reminding reader of the purpose of the study then identify the theory

Who coined the theoryDate theory was coined

Key constructs of the theorynote that you will incorporate the constructs into the interview questions later

how theory aligns to your purpose statement-Often you can find a theory that aligns to your study by reading dissertations like yours or going to google scholar or quicker yet – check with the librarian on theories that align to your topic

who else has used the theory in research = go to ProQuest Dissertations and type in the name of your theory and studies who have included the theory typically pop up. Then you can formulate a short story about the theory. For example, Jones (2025) used the XXX theory in a qualitative study with xxx participants in Central United States. Findings included xxxxxx.

This section should be 4-5 pages long with 5-8 references.

As always, before you submit to faculty, run your work through reciteworks.com and turnitin as auditors will do so.

The specific problem that is being investigated is the need to fill the leadership void in a general management problem in the financial field. Research question 1 aims to investigate the extent to which executives believe the ML technology is valuable and easy to use; research question 2 is focused on what strategies executives take into account when adopting ML technology, and research question 3 is aimed at what challenges executives might face when trying to implement the ML technology to be successful. TAM addresses the project questions immediately by providing constructs (PU and PEOU) to analyze the behaviors of managers when it comes to technology adoption. The present project adopts the TAM of Fred Davis to delve into the managerial processes of financial institutions in reviewing and shaping the ML technology for fraud detection. Working with the TAM model, the managers propose a strategic plan on the incorporation of the technology aimed at a change in organizational performance, a concern that is most relevant to general management decisions in the financial services industry.

The two similar constructs – PU and PEOU – are promoting the use of technology, whereas TAM is based on five basic constructs. The extent to which users perceive that a system will improve job performance is referred to as PU, and the extent to which users perceive that the system will be effort-free is referred to as PEOU. For the adoption of ML, PU can be associated with the improvement in fraud detection accuracy, operational effectiveness, and competitive edge (Ayodeji, 2024). PEOU is about how financial managers and staff can adopt and use ML systems. The factors are combined to impact the user attitude toward using technology, user behavioral intention to use technology, and ultimately system use.

The study uses TAM to try to understand why some ML technologies succeed and others fail and what the factors are that influence the success or failure of their implementation. Consequently, the framework closely aligns with the motivation of the project – to explore the

strategic structures for capitalizing on ML implementation in financial institutions. The theory is a solid base for the study of the cross-section of finance, technology and management strategy, making it appropriate for the DBA research level.

The project primarily uses the original TAM, but there are extensions to the model which provide valuable further information. For instance, TAM2 introduces other factors such as subjective norms and extends the PU with social influence and cognitive instrumental processes to better understand technology adoption in the organisation (Granić, 2024). Similarly, the Unified Theory of Acceptance and Use of Technology (UTAUT) combines elements such as performance expectancy, effort expectancy, social influence, and facilitating conditions for a broader context, including organizational and environmental factors (Zin et al., 2024). While the models proposed by TAM2 and UTAUT are not directly used in the project, the comprehensive aspects of the model affect the formulation of the questions for the interviews and the procedures for thematic coding in the data analysis. The relevance of TAM's constructs in solving the issue of slow and inefficient adoption of ML technology in financial institutions lies in the model's ability to predict key factors that impact organizational readiness and strategic fit. The project can discover the reasons behind the potential uptake of ML-based fraud detection systems by some financial institutions compared to others by investigating PU and PEOU. The results may have a direct impact on creating more effective approaches to the implementation of ML that are based on the context of the organization and the leadership's capacity.

In financial services, constructs like TAM have been employed to assess how effective the technology is in averting monetary losses as a result of fraud. So, the model aligns with the project's goal of understanding the financial manager's perspective on the value and usability of ML for fraud prevention and improving operations (Thathsarani & Jianguo, 2022). The TAM

approach is especially relevant to this research as it majors on user acceptance—a key factor in the failure of many strategic initiatives of ML in financial institutions. The TAM differs from technical models of technology implementation in that it emphasizes cognitive and behavioral aspects of technology adoption, which is in line with the orientation of the project toward managerial and leadership aspects.

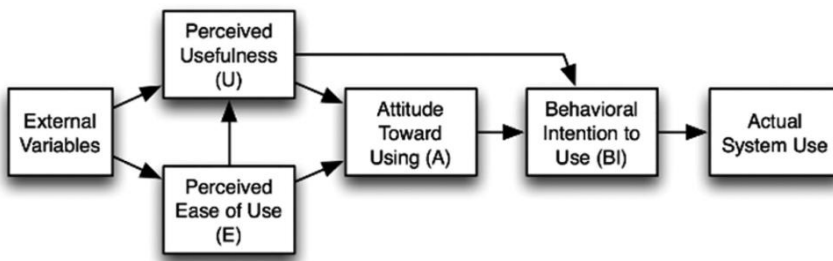
TAM will be used as a structure for the literature review, and it will be used as a systematic approach to structure and evaluate previous studies related to technology adoption in the financial sector. Regarding the application of the TAM theory, it is found that Thathsarani & Jianguo (2022) applied TAM theory in their qualitative study in the context of Small and Medium Enterprises (SMEs) in Sri Lanka with 487 participants. Results showed that digital use in the financial aspects, via the TAM, was a key factor in enhancing the performance of SMEs. Masumbuko & Phiri (2024) demonstrated the role of TAM and suggested the use of the framework in the enhancement of strategic management, technological capability, and user acceptance. The project's financial sector testing of TAM also makes the model applicable to a high-risk, high-compliance industry that faces a complex challenge in adapting to AI and ML technologies in the context of fraud detection systems. The project makes a contribution to the literature and presents context-specific findings on the perceptions and preparedness of the executive in relation to ML integration.

Once technology is applied to the management decision-making process at the strategic level, the gap between technological capability and the framework for management adoption of technology will be bridged. In doing so, the project will bring together practical and concrete steps for leadership to take in reducing fraud. Semi-structured interview questions will be formulated to elicit rich (qualitative) data from financial executives as a vehicle for data

collection, as guided by TAM. Attitudes (PU) and beliefs (PEOU) toward the usefulness of the ML for fraud detection will be explored along with other contextual factors such as regulatory pressures, organizational culture, and management support for integration. While analysis may consider information from models (e.g., TAM2, UTAUT) to further improve the results, the project will be based on a consistent theory by aligning constructs with those in the original TAM model.

Figure 1

Technology Acceptance Model for ML Integration in Financial Industry (Musa et al., 2024).



In the fifth phase of the project, which is Data Analysis, a qualitative thematic approach will be used to code the data that have been collected from the interviews with the managers of financial institutions. The initial code scheme will not explicitly be informed by constructs of the TAM, but it will use the TAM as a conceptual model in the interpretation of the emergent themes. The development of the project will involve analyzing common trends in leadership perspectives on the use of and tactical integration of ML systems for fraud detection (Masumbuko & Phiri, 2024). Therefore, it was decided that the TAM would be used for the project as it is relevant to the framework in relation to technology adoption in the organizational environment, particularly for financial environment managers to make strategic decisions. Financial organisations are under intense regulatory scrutiny, undergoing aggressive digital change, and being subjected to increased customer demands for security (Thathsarani & Jianguo,

2022). The TAM constructs offer a logical framework that helps to understand the TAM drivers in executive decision-making.

The project seeks to add to the literature in a number of important ways. Gradually, there is a need to provide an overview of the views of the financial managers on ML implementation strategies in the context of fraud detection and risk management (Pattnaik et al., 2024). Second, understanding the organizational attributes that have an impact on the adoption of ML, such as risk tolerance, regulatory compliance, technological infrastructure, etc., and leadership readiness. Third, exploring the alignment of TAM and the real-life TAM issues in ML-based anti-fraud systems in financial organizations (Gupta et al., 2025). The results of the project will be transferred into more effective plans on how to integrate ML and offer valuable, evidence-based tips for business decision-makers and financial industry regulators. The project will therefore investigate the relationship between technology acceptance and strategic leadership and thereby close the gap between theory and practice in financial management; and create value in technology integration for boosting the performance of organizations.

Project Context

Historical Background and Current Trends

Synthesis of the Scholarly Literature

Synthesis of the Practitioner Literature

Alignment of the Project With the Literature and Discipline

SECTION 2. PROCESS

Project Questions

Project Design/Method

Stakeholders, Participants, and Target Audience

Role of the Researcher

Project Study Protocol

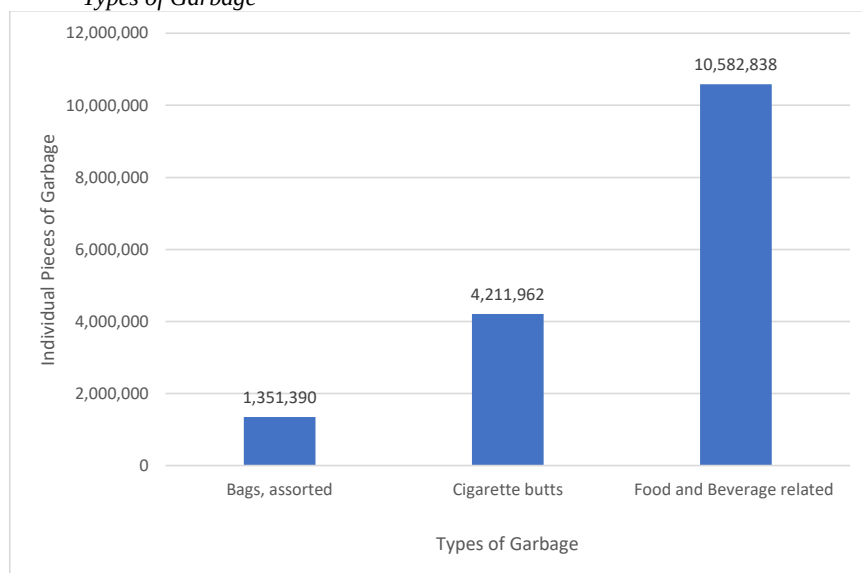
Sample

Data Collection

Ethical Considerations

Data Analysis

Figure 1
Types of Garbage



Note: Insert information about the source or presentation of the data if you did not create the figure. Add copyright/permission notes for copied information, even government materials, which require a 10-point acknowledgment below the image. Be sure to include a permission acknowledgment, e.g., “Reprinted [or adapted] with permission.” See the templates at <https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-28>.

Table 1
Demographic Information

Participant	Age	Sex	Position	Years in position
P1	25-30	Male	Chairman	10-15
P2	41-45	Female	CEO	6-10

Note. Potential participants under age 16 were omitted from the sample. Only essential notes need to be included. See [Table setup \(apa.org\)](https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-44?group=All&view=list&term=tables&sort=asc) and <https://academicwriter-apa-org.library.capella.edu/learn/browse/QG-44?group=All&view=list&term=tables&sort=asc>. The [Doctoral Publications Guidebook](#) also addresses tables and figures.

SECTION 3. FINDINGS AND APPLICATION

Relevant Outcomes and Findings

Application and Benefits

Implications

Recommendations for Policy

Recommendations for Practice

Recommendations for Future Work

Conclusion

References

- Abikoye, N. B. E., Akinwunmi, N. T., Adelaja, N. A. O., Chidozie, S., & Ogunsuji, M. (2024). Real-time financial monitoring systems: Enhancing risk management through continuous oversight. *GSC Advanced Research and Reviews*, 20(1), 465-476. <https://doi.org/10.30574/gscarr.2024.20.1.0287>
- Afjal, M., Salamzadeh, A., & Dana, L. P. (2023). Financial fraud and credit risk: Illicit practices and their impact on banking stability. *Journal of Risk and Financial Management*, 16(9), 386. <https://doi.org/10.3390/jrfm16090386>
- Ayodeji, I. (2024). *Forensic accounting and fraud prevention and detection in the Nigerian banking industry*. Proquest.com. <https://www.proquest.com/openview/aca05307a360975338fe59b6a3b0c74b/1?cbl=18750&diss=y&pq-origsite=gscholar>
- Bevilacqua, S., Masárová, J., Perotti, F. A., & Ferraris, A. (2025). Enhancing top managers' leadership with artificial intelligence: Insights from a systematic literature review. *Review of Managerial Science*. <https://doi.org/10.1007/s11846-025-00836-7>
- Borhani, S. A., Babajani, J., Vanani, I., Anaqiz, S., & Jamaliyanpour, M. (2021). Adopting blockchain technology to improve financial reporting by using the technology acceptance model (TAM). *International Journal of Finance & Managerial Accounting*, 6(22), 155–171. http://www.ijfma.ir/article_17481.html
- Brogi, M., & Lagasio, V. (2024). New but naughty. The evolution of misconduct in FinTech. *International Review of Financial Analysis*, 95, e103489. <https://doi.org/10.1016/j.irfa.2024.103489>
- Chenguel, M. (2020). Financial fraud and managers' causes and effects. *Corporate Social Responsibility*. <https://doi.org/10.5772/intechopen.93494>
- CIO. (2024). *Banks and lenders are still falling short of fully capitalizing on the AI revolution*. Cio.com. <https://www.cio.com/article/3513901/banks-and-lenders-are-still-falling-short-of-fully-capitalizing-on-the-ai-revolution.html>
- Dama, K., Reddy, K., Hrithik, K., Raheem, D., & Vyshnavi, K. D. (2024). *Fraud detection in financial transactions*. Researchgate.net. [https://www.researchgate.net/publication/379654286_Fraud_Detection_in_Financial Transactions](https://www.researchgate.net/publication/379654286_Fraud_Detection_in_Financial_Transactions)
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319–340. <https://www.jstor.org/stable/249008>
- Davis, F. D., & Granić, A. (2024). *The technology acceptance model*. Springer.com. <https://link.springer.com/book/10.1007/978-3-030-45274-2>

Commented [Dr. T3]: Receiteworks.com flagged this – you need initials for this last author.

- Ebot, A. (2024). *Technology acceptance model for adopting cybersecurity technology in small and medium business/enterprise: A generic qualitative study*. Proquest.com. <https://www.proquest.com/openview/821ddca62bfb9689de0e377a43f7dfba/1?cbl=18750&diss=y&pq-origsite=gscholar>
- Federal Trade Commission. (2025). *New FTC data show a big jump in reported losses to fraud to \$12.5 billion in 2024*. Ftc.gov. <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
- Feingold, S., & Wood, J. (2024, April 10). “Pig-butcher” scams on the rise as technology amplifies financial fraud, INTERPOL warns. Weforum.org. <https://www.weforum.org/stories/2024/04/interpol-financial-fraud-scams-cybercrime/>
- Granić, A. (2024). User acceptance of interactive technologies. *Foundations and Fundamentals in Human-Computer Interaction*, 356–389. <https://doi.org/10.1201/9781003495109-12>
- Gupta, R. K., Hassan, A., Majhi, S. K., Parveen, N., Zamani, A. T., Anitha, R., Ojha, B., Singh, A. K., & Muduli, D. (2025). Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach. *Results in Engineering*, 26, e105084. <https://doi.org/10.1016/j.rineng.2025.105084>
- Hariyani, D., Hariyani, P., Mishra, S., & Sharma, M. K. (2024). Causes of organizational failure: A literature review. *Social Sciences & Humanities Open*, 10, e101153. <https://doi.org/10.1016/j.ssaho.2024.101153>
- Hilal, W., Gadsden, S. A., & Yawney, J. (2021). A review of anomaly detection techniques and applications in financial fraud. *Expert Systems with Applications*, 193(1), e116429. <https://www.sciencedirect.com/science/article/pii/S0957417421017164>
- Joseph, P. S., & Eaw, H. C. (2023). Still technology acceptance model reborn with exostructure as a service model. *International Journal of Business Information Systems*, 44(3), 404–421. <https://doi.org/10.1504/ijbis.2023.134949>
- Lamey, Y. M., Tawfik, O. I., Durrah, O., & Elmaasrawy, H. E. (2024). Fintech adoption and banks’ non-financial performance: Do circular economy practices matter? *Journal of Risk and Financial Management*, 17(8), 319. <https://doi.org/10.3390/jrfm17080319>
- Masumbuko, C., & Phiri, J. (2024). Technology adoption as a factor for financial performance in the banking sector using UTAUT model. *African Journal of Commercial Studies*, 4(2), 121–130. <https://doi.org/10.59413/ajocs/v4.i2.5>
- McKinsey & Company. (2022). *Four key capabilities to strengthen a fraud management system* | McKinsey. Mckinsey.com. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/four-key-capabilities-to-strengthen-a-fraud-management-system>
- Musa, H. G., Fatmawati, I., Nuryakin, N., & Suyanto, M. (2024). Marketing research trends using technology acceptance model (TAM): A comprehensive review of research (2002–

2022). *Cogent Business & Management*, 11(1).
<https://doi.org/10.1080/23311975.2024.2329375>

Pattnaik, D., Ray, S., & Raman, R. (2024). Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review. *Heliyon*, 10(1), e23492.
<https://www.sciencedirect.com/science/article/pii/S2405844023107006>

Statista. (2025). *Value of fraud loss in the U.S. by payment method 2021*. Statista.com.
<https://www.statista.com/statistics/958997/fraud-loss-usa-by-payment-method/>

Thathsarani, U. S., & Jianguo, W. (2022). Do digital finance and the technology acceptance model strengthen financial inclusion and SME performance? *Information*, 13(8), 390.
<https://doi.org/10.3390/info13080390>

Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. *Financial Innovation*, 9(1).
<https://doi.org/10.1186/s40854-023-00470-w>

Zin, R., Mokhtar, N., Irfan, A., Ani, C., Husairi, A., Nasrun, M., & Nawi, M. (2024). Unraveling the dynamics of user acceptance on the Internet of Things: A systematic literature review on the theories and elements of acceptance and adoption. *Journal of Electrical Systems*, 20(4), 2217–2227.
<https://pdfs.semanticscholar.org/b422/8ae2ee05db93a186f3ca6f2976741c032fec.pdf>

APPENDIX A. TITLE OF APPENDIX A

Format titles as shown here. Do not include recruitment flyers, permissions correspondence, invitations to subject matter experts, or informed consent forms. They should be removed before submission to the committee and doctoral publications review. Place tables and figures in the sections at the point where they are discussed.

ONCE YOU'VE WRITTEN THE APPENDICES, DELETE ALL INSTRUCTIONS.

DELETE THIS PAGE IF NOT USED.

APPENDIX B. TITLE OF APPENDIX B

Format titles as shown here. Do not include recruitment flyers, permissions correspondence, invitations to subject matter experts, or informed consent forms. They should be removed before submission to the committee and doctoral publications review. Place tables and figures in the sections at the point where they are discussed.

ONCE YOU'VE WRITTEN THE APPENDICES, DELETE ALL INSTRUCTIONS.

DELETE THIS PAGE IF NOT USED.