STRATEGIES FOR IMPLEMENTING MACHINE LEARNING FRAUD DETECTION IN THE U.S. FINANCIAL INDUSTRY

by

Student name

DB-FPX8840

Professor name

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

Abstract

The purpose of the abstract is to provide a concise and accurate synopsis of key elements of your capstone project. Set the abstract as a single block-style paragraph with no initial indent. Address the following topics (400 words maximum). **Research topic summary (1-5 sentences),** a concise summary of your capstone research topic. Explain the rationale for your study and the need for the study the capstone addresses. Indicate your research questions, matching the wording used in your capstone sections. **Research Methodology (1-2 sentences).** Summarize the research methodology used in the study. **Population and sample (1-2 sentences).** Describe the population and sample, including high-level demographic information regarding your participant pool. If secondary data were used, describe the data set. **Data analysis (1-2 sentences)** provides a concise summary of your data analysis. **Findings (1-3 sentences)** Provide a concise summary of your research findings and conclusion(s). Describe the practical implications of your project and the deliverable you created.

Tips for Developing a Quality Abstract. (a) The abstract is representative of your work. Researchers will review your abstract to determine whether your manuscript is worthy of reading and relevant to their literature review. Those in your field will review your abstract to learn more about the nature and quality of your doctoral work. Thus, the abstract stands as a record of your doctoral-level work. (b) Additional guidelines for development of an abstract are in section 3.3 of the *APA Publication Manual*, 7th edition, or on Campus at Academic Writer, 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. Format the abstract as one double-spaced block-style paragraph (i.e., do not indent the first line). Set the text flush left, ragged right. Do not justify the right margin. Do not use 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 optional. It is your acknowledgment indicating your appreciation and respect for significant individuals in your life. The dedication is personal; thus, any individuals named are frequently unrelated to the topic of the capstone.

Typically, learners dedicate the work to the one or two individuals who instilled the value of education and the drive to succeed in educational pursuits. Learners often dedicate capstones to relatives, immediate family, or significant individuals who have supported them or played a role in their lives.

Avoid identifying participants or anyone connected with the research site. You may use individuals' titles with no name (e.g., "Thanks to the research director and site proctor for their help"). Or you may name individuals without connecting them to the site (e.g., "Thanks to Abdul Ibrahim and Mary Carson for their help"). Typically, avoid naming 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 acknowledgments page is optional. The acknowledgments differ from the dedication in that they recognize individuals who have supported your scholarly efforts related to the advanced doctoral manuscript or who have held a role in your academic career as it relates to the research of the advanced doctoral manuscript. This might mean a mentor and committee members, advisor, online or colloquia faculty, and other support people from Capella or other organizations. If you received financial support from fellowships, grants, or other organizational support, note it in this section. The acknowledgments are also appropriate for thanking statisticians, transcriptions, those who have provided permission to use an instrument, and the like.

Avoid identifying participants or anyone connected with the research site. You may use individuals' titles with no name (e.g., "Thanks to the research director and site proctor for their help"). Or you may name individuals without connecting them to the site (e.g., "Thanks to Abdul Ibrahim and Mary Carson for their help") Typically, avoid naming the site. Learners often thank those who have provided permission to use an instrument.

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

Table of Contents

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

List of Tables

ONCE YOUR LIST IS COMPLETED, REMOVE INSTRUCTIONS

AND UPDATE THE PAGE NUMBERS.

DELETE THIS PAGE IF NOT NEEDED.

List of Figures

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

In an age of technological progress, we're as easy as ever to do financial transactions, and so is the size of financial fraud in the United States. Whether it's ATM fraud, credit card fraud, identity theft schemes, wire transfer fraud, or account takeovers, it's common knowledge that fraud schemes are getting increasingly sophisticated, and financial services institutions are meeting the challenge. In addition, American consumers reported the lowest amount of credit card fraud in the third quarter of 2024, at just about $58 million in dollars (Statista, 2025). The number highlights the imperative need for smarter and more responsive fraud detection systems that can detect and prevent illegal activities in real time.

Current fraud detection methods rely on manual decision making and pre-defined rules, and may not be able to respond to new and developing challenges in fraud posing in the financial services. With the advent of new technologies such as Artificial Intelligence (AI) and machine learning algorithms, there are opportunities to develop more sophisticated and adaptive algorithmic fraud detection strategies. Not all financial institutions (CIO, 2024) are making full use of AI technologies to detect fraud. In fact, in the face of increasingly sophisticated fraud schemes, organizations will need to do more than simply rely on technology and introduce more of a management-driven approach to innovation. Despite the need for better fraud detection, many organisations struggle with technology issues, organizational silos, and management risk and know how gaps that prevent them from implementing better fraud detection. The challenges underline a lack of practice by general managers, who don't have a clear plan on how to integrate AI strategic and operational frameworks within institutions.

A major challenge in the financial industry, including the U.S., in an era of growing digital financial transactions by financial institutions like banks or financial technology (fintech) firms (Brogi & Lagasio, 2024), is fraud. While these payment systems are convenient to use, they don't have enough time to manually intervene against fraud (Vanini et al., 2023). But there is a huge expectation upon institutions to implement an effective fraud detection system that can identify anomalies, trigger an alarm on questionable transactions, and act automatically almost instantly (milliseconds). Business goals aligned with machine learning capacities reduce fraud in financial institutions by a huge margin, according to Abikoye et al (2024). The importance of managerial skills and preparedness in fully achieving the value of machine learning initiatives was highlighted by Bevilacqua et al. (2025). The organizational efforts have an important role to play in the long-term success regarding the activities of fraud detection and limit risk exposure.

The machine learning algorithms would be used to detect fraudulent activities at financial institutions in the U.S. Anomaly detection in machine learning would enable financial institutions to implement an effective fraud prevention system, recognizing fraudulent activities (Dama et al., 2024). The underlying issue at hand is the lack of leadership approaches in the context of implementing machine learning in financial institutions for addressing fraud operations (Gupta et al., 2025). The issue here is that many financial institutions have a management that doesn't possess the advanced procedures and operations required to combat financial fraud using advanced technologies such as machine learning (Chenguel, 2020). However, once a technological solution has been identified, the challenge lies in the managerial process for the uptake of the solutions and getting them to become part of the organisational processes and decision-making systems. The project's potential impact is the ability of financial entities to gain recognisable benefits and the creation of a more secure financial system offering consumers protection from fraudulent transactions, through active fraud identification and prevention.

Financial institution managers may have a new piece of knowledge or information resulting from the significance of the proposed project that helps them pinpoint fraud earlier to minimize the financial losses. This adoption of machine learning technology is aided by effective leadership practices, enabling proactive detection of fraud events and reducing them to a minimum (Bevilacqua et al., 2025). So, machine learning can contribute to combating brand new frauds and improving the health of the organisation's finances. For this reason, the problem that will be addressed by the project will be sudden and disappointing deployment and administration of smart fraud detection systems by a business. Focusing on managerial aspects of integrating machine learning technology, the data from this project may provide a way forward for financial institutions interested in updating fraud prevention measures to guarantee long-term security and confidence in the digital world.

Problem Statement and Purpose

The overall business issue is that fraud incidents lead to loss in both profitability and customer satisfaction in the U.S. financial industry (Shi et al., 2023). Traditional fraud detection systems can't detect fraud and affect the organization's performance. The Federal Trade Commission (FTC) reports that Americans lost $90 to $501 million from fraud in the United States in 2025. The increasing losses reveal that fraud is not only a continual problem, but it's also becoming more sophisticated, and it is a threat to consumer trust and organizational stability.

The specific business problem is that some technology managers in the U.S. financial industry do not have the effective resources and technology strategies to implement machine learning-driven fraud protection (Bello & Olufemi, 2024). While financial institutions have access to advanced technologies, a lot of times leadership flaws, failure to receive strategic support, or other reasons make it difficult to implement a fraud detection system, impacting organizational performance (Afjal et al., 2023). Around 2.6 million consumers have reported fraud as a result of misaligned leadership by consumers, saying they needed more leadership in integrating advanced technology (FTC, 2025). The effects of this particular business challenge are multifaceted, leading to increased vulnerability to fraud, loss of customer confidence, and significant financial losses (Lamey et al., 2024). Keeping up with the gap between technology and strategic leadership issues is one of the most important problems in the context of financial industry management.

Alignment with Program

A Doctor of Business Administration (DBA) project on leveraging machine learning technology with strategic leadership in financial institutions is a perfect match because the project is aimed at solving a high-impact business problem, and it is focused on the financial industry. Financial fraud continues to be a major problem in the financial services industry in terms of both expenses and complexity (Hilal et al., 2021). So the project is about the operators and operator failures at the strategic level that prevent the machine learning and therefore cause financial losses, regulatory risk, and/or reputational damage. The Journal highlighted the significance of the role that leadership can play in enhancing financial operations by incorporating machine learning technology. Therefore, this proposed project is a good match for the Doctor of Business Administration (DBA) emphasis in interdisciplinary leadership and strategic management. Exploring the financial manager's capability to make the decisions to implement advanced technology provides valuable insights into improving the operations financially in an organization and reducing the risk of fraud (Dama et al., 2024). The work of the project in the DBA is based on the problem-solving process, doing research related to the business applications.

Purpose Statement

The proposed generic qualitative inquiry aims to elicit the views of technology managers in the financial industry who have thus far adopted resources and technology strategies to combat machine learning-driven fraud detection and protection in the U.S. financial sector. The proposed project will delve into the concepts of Leadership strategy in the adoption of machine learning technology for fraud detection (Dama et al., 2024). The target population will be financial managers in U.S. financial service institutions in the U.S.

Gap in Practice

The difference is that some U.S. financial industry managers still haven't embraced effective machine learning-driven strategies to minimize fraud detection failures, which leads to continued financial losses and customer dissatisfaction (Chen et al., 2025). According to the statistics from the Federal Bureau of Investigation, BEC attacks increased in 2022 from 17,348 in 2021 to 21,832 attacks, resulting in losses of approximately $2.7 billion (Lalchand et al., 2024). Fraud detection using standard systems is not keeping up with the changing methods of fraudsters and tends to be fraudulent. The practice gap is not an issue associated with the unavailability of fraud detection technologies but due to a lack of a leadership strategic approach to implement the machine learning technology (Hariyani et al., 2024). The disparity means the specific problem that financial institutions face is that of being vulnerable to fraud tactics that cannot be detected by existing systems, leading to monetary loss. The ideal state is when managers of financial institutions are actively leveraging the predictive power of machine learning, real-time identification of fraudulent activities, and high accuracy in detecting and preventing fraud (Pattnaik et al., 2024). The findings from the project may be helpful to practitioners who are looking to narrow the gap and understand that the use of more advanced analytical techniques in the fight against fraud can be useful. Besides, the outcome should be considered as part of a business's general strategic plan.

Theoretical Framework

The work investigates the opinions of U.S. financial technology (FinTech) Managers using resource and technology measures of those who have adopted ML technology (machine learning) in fraud detection and protection. The qualitative research study was practically oriented, where the technology acceptance model (TAM) was originally developed by Davis (1989). The TAM has been adopted as a popular explanatory model of the adoption of emerging technologies. It continues to be highly relevant in the study of strategic, behavioral, and managerial issues in the implementation of machine learning in financial institutions (Davis & Granić, 2024). The theoretical basis offers valuable insights into the intricate decision-making processes leading to effective technology integration in high-stakes financial contexts.

Perceived usefulness at a manager level reflects what managers think the machine learning systems have the potential to achieve in terms of better fraud detection results and adding value to the organisation. The ease of use signifies the degree to which managers believe that the implementation of machine learning systems will not be complex and demanding excessive effort for financial organizations (Joseph & Eaw, 2023). Perceived ease of use may shape managers' attitudes toward ML adoption, especially if others in an organization are reluctant to adopt ML because of their perceived difficulties in implementing it. The sequential technology acceptance model constructs of attitude towards use, intention to use behavior, and actual system use offer a systematic framework to understand how managers form perspectives, develop intention, and finally adopt machine learning technology.

The TAM is one of the most-used models for explaining the adoption of new technologies, especially within an organizational context, in general management literature. According to the TAM, two main factors that affect the acceptance of a technology are its ease of use (EU) and usefulness (U). The TAM is an appropriate model for the project because it allows for an explanation of how financial managers at U.S. financial institutions might or might not implement machine-learning-based fraud-detection systems, especially given the seemingly clear advantages of these technologies.

An important secondary model is the unified theory of acceptance and use of technology (UTAUT), which is an extension of TAM, adding constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. (Borhani et al., 2021) By adopting this framework, both scholars and practitioners it helps to have a more nuanced perspective of technology adoption in organizations. For the project, the other variables will be used to understand the factors outside of the manager's influence that could affect their decision to implement machine-learning-based fraud-detection systems, including the organizational culture, leadership support, and training.

The focus of the specific problem explored is to understand the managerial perspectives in the context of the technology acceptance model. The research questions are laid out to explore perceived usefulness and ease of use, which shape executives' perceptions of machine learning technology adoption, what drivers would trigger behavioral intentions, and what impediments would exist for implementing the system. The proposed project questions can be directly mapped to the TAM for constructs (perceived usefulness and perceived ease of use), which can be explored while focusing on the decision-making views of managers in the adoption of a technology. The conceptual framework to understand the attitude of financial institutions' managers towards the machine learning technology that is used to detect fraud is one of the conceptual frameworks employed in the current project, which is called the TAM by Fred Davis (Pajany, 2021). The basic constructs of the TAM model directly impact the attitude formation process (Borhani et al., 2021). The strategic approach to the use of technology that the TAM model of perspective towards the new technology directly corresponds to the result of the performance of the organization. Therefore, the framework is quite applicable in forming the thinking on management decision- making, mainly in financial services.

The TAM is based on five constructs; perceived usefulness and perceived ease of use are the two most important constructs to predict the acceptance of technology. Perceived usefulness indicates the user's perception of the system's usefulness for improving job performance. The perceived usefulness is associated with how managers and senior management form thoughts on how increased accuracy in fraud detection, efficiency in operations, and improvement in competitive edge can be achieved. The constructs impact users' attitudes towards the technology, the intention to use the technology, and the actual use of the system. Perceived ease of use shows the financial managers' perceptions of the availability and ease of use of the machine learning system. These constructs have an impact on the attitude towards technology, the attitude towards intent to use technology, and system use of the user of technology.

The study examines the relationship between managerial attitudes and perceptions of strategic readiness to adopt machine learning technology and the constructs of TAM and its potential for successful adoption of the technology, and support from organisations. The framework allows for the proposed project to consider the the manager's's perspective. This framework directly contributes to the concept of the project to analyze the perception of managers concerning ML in financial institutions. This means that the fusing of the worlds of finance, technology, and management also represents a theoretical lens and that the DBA-level research that focuses on understanding the processes of technology adoption decision-making could be relevant to consider.

Though the main model that is utilized in the project is the original TAM, the extension of the model provides TAM that considers additional variables like subjective norms and expounds the perceived usefulness via the social influence and cognitive instrumental action, improving the comprehension of organizational technology adoption standpoints (Granić, 2024). In the same way, the unified theory of acceptance and use of technology (UTAUT) combines the constructs, such as performance expectancy, effort expectancy, social influence, and facilitating conditions. The model likely has a wider scope in terms of the range of factors impacting organizational and environmental perspectives on adoption (Zin et al., 2024). While TAM2 and UTAUT will not be used as the main framework, the extended constructs of the models will be used for the development of interview questions and the thematic coding procedures in data analysis.

The significance of the TAM for the study of the slow technology adoption of machine learning in the financial sector is that it is a model that enables the prediction of important factors that influence managers' adoption perspectives and strategic alignment. The project will analyse TAM to identify common reasons for some financial institutions to be more amenable to machine learning-based fraud detection systems when compared to others. The results can be translated into how to implement machine learning in more effective ways in accordance with the management perspectives and organizational contexts.

In other business areas, such as social or information and communications technology (ICT), TAM and extended constructs have been used to determine technology adoption views on fraud prevention effectiveness. The framework aligns with the proposed project's goal of examining financial managers' views on the value and accessibility of machine learning in fraud prevention and operational efficiency. TAM is highly relevant to the investigation as the model focuses on the user perspective on acceptance, a key factor in the challenges faced by strategic investments in machine learning in financial institutions (Rawindaran et al., 2021). TAM does not address technical implementation models but rather focuses on the cognitive and behavioral parts of perspectives on adoption, in parallel with the managerial focus of the project.

The TAM gives a structure to follow when doing a literature review and is a systematic method of organizing and comparing studies of TAM and the views on technology adoption in financial sectors. Thathsarani and Jianguo (2022) conducted a qualitative study with 487 Small and Medium Enterprises (SMEs) in Sri Lanka, and they found that from SMEs' perspective on digital adoption with the TAM lens, digital adoption is around financial context and significantly impacts the performance of SMEs. The scholars also showed that financial organisations are under regulatory pressure, have a strong drive to move fast toward digital transformation, and their customer security requirements are ever-growing, all of which affect the evaluation of potential technologies to be adopted by managers. However, Masumbuko and Phiri (2024) showed TAM application and called for the adoption of the framework for improving the strategic management, technological capability and user acceptance perspectives.

The project introduces a new perspective of the TAM model, applicable to the fraud detection systems in the financial industry, where the adoption of AI and machine learning is both important and complicated. The project makes a research contribution by providing insights on executive perspectives and readiness for integration of machine learning around a specific context.

The shift from the technology acceptance at the user level to the managerial perspective in the analysis of TAM application will fill the technological capability and adoption of decision-making frameworks. The proposed project aims to provide actionable strategies with regards to effective fraud reduction – via the lifting of managerial perspective to match technology potential. The TAM will be used to develop semi-structured interview questions that would elicit rich, qualitative responses from the financial executives on issues pertaining to the perspectives on Machine learning adoption (Ebot, 2024). Questions will focus on attitudes towards usefulness of machine learning for fraud prevention, expectations of ease/difficulty of integration, and other contextual factors such as regulatory pressures, organizational culture and leadership buy-in that may impact views on integration. Depending on the model used (such as TAM2 or UTAUT), the constructs in this project are based in the original TAM model in order to keep the theory consistent, but should also be considered for addition into the analysis.

In the Data Analysis phase, financial institution managers' data will be coded using qualitative and thematic approaches. Although TAM constructs will be not explicitly specified in coding frameworks, these might be conceptual models from which to better understand emergent themes involving adoption perspectives. The project will analyse the commonalities in management attitudes in the process of the adoption and the strategic integration of machine learning systems for fraud detection (Masumbuko & Phiri, 2024). The TAM in the usage instrument was chosen because it represents technology adoption perspectives as it relates to technology usage within an organizational context, especially in the financial organization where managers make strategic decisions regarding technology. Regulatory oversight, upbeat digital change, and rising customer security requirements are all exerting pressure on financial companies' capacity to evaluate potential for new technology adoption by their managers.

The project data can have a number of contributions to the literature. The data will reflect financial managers' attitudes towards strategies for implementing machine learning in fraud detection and risk management, first. Second, the study will take a look at the organizational factors that influence machine learning adoption perspectives such as risk tolerance, regulatory compliance, technological infrastructure and managerial readiness. Third, the alignment between constructs of TAM and the real-world challenges of implementing machine learning in financial fraud prevention settings will be explored (Gupta et al., 2025). Study data might be utilized to understand better how to promote more effective strategies for the adoption of machine learning by practitioners and policymakers. The project may help to bridge existing theory-practice gaps in financial management, working to better use and choose technology to enhance performance in organizations, with a focus on managerial perspectives of technology adoption.

.

.

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

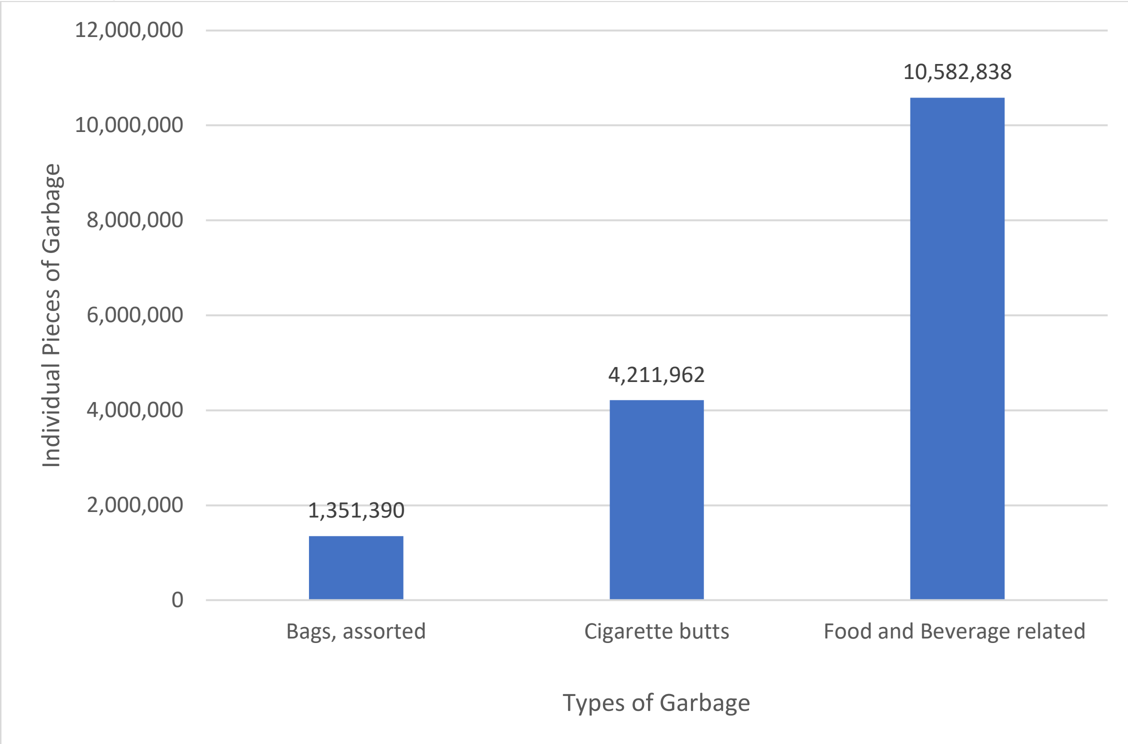
Data Collection

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) 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*. 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*. 1-37. 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 (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., Pavan, K., Hrithik, K., & Vyshnavi, R. (2024). Fraud detection in financial transactions. *ResearchGate.com*. https://doi.org/10.13140/RG.2.2.33977.99685

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. https://link.springer.com/book/10.1007/978-3-030-45274-2

Ebot, A. (2024). *Technology acceptance model for adopting cybersecurity technology in small and medium business/enterprise: A generic qualitative study.* 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-butchering" 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, the 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

Pajany, P. (2021). *Ai transformative influence: Extending the tram to management student's AI's machine learning adoption - ProQuest*. Proquest.com. https://search.proquest.com/openview/317b9e11c91c8b592822e9cb42b758ba/1?pq-origsite=gscholar&cbl=18750&diss=y

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

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150. https://doi.org/10.3390/computers10110150

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). 66. 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 committee and the 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 committee and the 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.