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

by

Student Name

DB-FPX8840

Professor Name

Maja Zelihic, 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

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

The digital age has been followed by an age of never-before-seen convenience in financial transactions; however, it has also increased the magnitude of financial fraud in the United States. The financial sector is constantly fighting against increasingly complex kinds of frauds, from credit card scams, identity thefts, wire transfer frauds and account takeovers (Afjal et al., 2023). Further, American consumers filed approximately $58 million worth of credit card fraud in the third quarter of 2024, which was the lowest reported amount for that year (Statista, 2025). The number testifies the imperative need for more intelligent and more responsive fraud detection systems to detect and prevent illegal activities in real-time.

Existing approaches to fraud detection are generally based on human judgment and pre-programmed rules, which may not be able to respond to the new threats of fraud in financial organizations. Emergent technological development, including the use of artificial intelligence (AI) and machine learning algorithms, offer potential for the building algorithmic fraud detection approaches that are more advanced and responsive (Pattnaik et al., 2024). Some financial institutions are not fully leveraging artificial intelligence to combat fraud (CIO, 2024). As fraud schemes become more sophisticated, organizational managers must look beyond technological solutions and adopt a management-oriented approach to innovation (McKinsey & Company, 2022). Despite advancements in technology, organizational resistance, unclear leadership, and poor cross-functional alignment are often the reasons for the underutilization of fraud detection tools. The challenges point to a gap in practice: many general managers do not have a clear roadmap for integrating AI's strategic and operational frameworks within institutions.

The U.S. financial industry, including banks and financial technology (fintech) companies, is highly vulnerable to fraud due to the volume and speed of digital transactions (Brogi and Lagasio, 2024). Real-time payment systems, on the one hand, while being convenient, leave little scope for manual intervention against fraud (Vanini et al., 2023). Institutions are under severe pressure to implement a fraud detection system that works and can detect anomalies, highlight suspicious behavior, and initiate automated responses within milliseconds. Abikoye et al. (2024) reported that strategic alignment between machine learning capabilities and organizational goals is very useful for reducing fraud incidents experienced by financial institutions. Bevilacqua et al. highlight the importance of managerial capability and organizational preparedness in achieving the business value of machine learning initiatives. Organizational efforts are key to the the long-term success of fraud detection initiatives and to minimizing risk exposure.

The project objective is to use machine learning algorithms to detect fraudulent activities in US financial institutions. The anomaly detection capabilities of machine learning will enable managers to use an efficient fraud detection system to identify fraudulent activities (Dama et al., 2024). The root problem identified is the need for leadership strategies to implement machine learning technology to combat fraud in financial institutions (Gupta et al., 2025). The challenge is that management in financial institutions typically lacks the strategic thinking and operational models to use state-of-the-art technologies, such as machine learning, to effectively address financial fraud (Chenguel, 2020). In the case of technologies, the disconnect in practice lies in the managerial capacity to embed solutions into organizational practices and decision-making systems. The project's significance is to provide substantial benefits to financial organizations and make the financial system safer for consumers by actively identifying and preventing fraudulent transactions.

The significance of this project may provide new insights for managers of financial institutions, helping them reduce economic losses by enabling them to detect fraud faster and more accurately. The application of effective leadership strategies will ensure the implementation of machine learning technology, which helps in the reduction of the occurrence of fraud events by being proactive in detecting them (Bevilacqua et al., 2025). Thus, building a culture of innovation with the help of machine learning would help address new fraud threats and ensure the organization's financial stability. Therefore, this project focuses on a business issue in general management: the ineffective deployment and administration of innovative fraud detection systems. Focusing on the managerial aspect incorporating machine learning technology. With data coming from this project, there may be a way forward for financial institutions to update their fraud prevention measures to ensure long-term security and confidence in the digital world.

Problem Statement and Purpose

The general business problem is that fraud incidents reduce profitability and customer satisfaction in the U.S. financial industry. Traditional fraud detection systems are not effective at detecting fraud and can impact organizational performance. According to the Federal Trade Commission (FTC),, the amount of money lost by U.S. consumers due to fraudulent activities was $90 to $501 million (FTC, 2025). The growing losses mean that fraud is not only here to stay but also becoming more complex, presenting a serious and ongoing threat to consumer trust and organisational stability.

The particular business problem, however, is the lack of adequate resources and technology strategies among technology managers in the US financial industry to enable the implementation of machine-learning-driven fraud protection (Bello and Olufemi, 2024). Despite the availability of advanced technologies, poor leadership and a lack of strategic support have been the leading factors in the failed implementation of fraud detection systems, which negatively affect organizational performance (Afjal et al., 2023). Leadership gaps in integrating complex technologies have been a major problem, with approximately 2.6 million consumers reporting fraud due to misaligned strategies (FTC, 2025). This particular business problem leads to several negative consequences, including prolonged exposure to fraudulent activity, loss of customer confidence, and significant financial losses (Lamey et al., 2024). A consistent relationship between technological capabilities and strategic leadership is a key issue in the broader context of financial industry management.

Alignment with Program

The project on leveraging machine learning technology through strategic leadership in financial institutions is a great fit for a Doctor of Business Administration (DBA), as it aims to solve an impactful business problem in the finance industry. Financial fraud is one of the costliest and most sophisticated problems in the banking and financial services industry (Hilal et al., 2021). Thus, the project intends to examine failures in strategic management as a contributor to the unsuccessful adoption of machine learning,, resulting in financial losses, regulatory risks, and reputational damage. The issue highlighted the importance of how leadership can assist in improving financial operations by integrating machine learning technology (Pattnaik et al., 2024). Thus, the project is a very good match for the Doctor of Business Administration (DBA) emphasis on interdisciplinary leadership and strategic management. Exploring the financial manager's ability to decide whether to implement advanced technology provides crucial insights into how to improve an organization's financial operations and reduce the risk of fraud (Dama et al., 2024). The project under the DBA focuses on solving complex problems in the business world through applied research.

Purpose Statement

The goal of this generic qualitative inquiry is to understand the perspectives of technology managers in the US financial industry who have implemented resource and technology strategies to support machine-learning-based fraud detection and protection. The project will discuss leadership strategies for adopting machine learning for fraud detection (Dama et al., 2024). The target population will include financial managers in the United States who work at institutions that serve the banking and financial services industry.

Gap in Practice

The difference in practice is that some managers in the U.S. financial industry have not adopted effective machine learning-based fraud detection, resulting in ongoing financial losses and customer dissatisfaction (Chen et al., 2025) as the statistics of the Federal Bureau of Investigation shows that the number of cases of business email fraud in 2022 increased up to 21,832 cases that resulted in losses of $2.7 billion (Lalchand et al., 2024). Not using standard systems to detect fraud, which is not keeping up with the evolving ways fraudsters operate and tends to lead to fraudulent activity. The reason for the practice gap is not the unavailability of fraud detection technologies but the lack of a strategic leadership approach to implement machine learning technologies (Hariyani et al., 2024). The gap is manifested as a particular issue: financial institutions are subjected to complex financial fraud schemes that remain undetected by existing systems, resulting in monetary losses. An ideal state is one in which the managers of financial institutions actively use the predictive power of machine learning systems to detect and prevent fraud in real time with high precision (Pattnaik et al., 2024). Project findings can help practitioners interested in closing the gap by highlighting the potential value of adopting more sophisticated analytical methods to prevent fraud. In addition, results must be taken in the context of a firm's overall strategic plan.

Theoretical Framework

The research focuses on views from the US financial sector technology managers who have adopted machine learning (machine learning) based fraud detection and protection systems by the application of resources and technology measures. The qualitative research study was practical based on the technology acceptance model (TAM) that was first developed Davis (1989). The TAM has gained wide popularity to explain the adoption of emerging technologies. The framework remains a powerful tool in the research on the strategic, behavioral, and managerial aspects of machine learning adoption in financial institutions (Davis & Granić, 2024). The theoretical foundation provides critical understandings of the complex decision making processes that contribute to the successful integration of technology in high stakes financial environments.

At manager level, perceived usefulness is what managers think the machine learning systems might possibly do to enhance the outcome of fraud detection and provide strategic organizational value. Perceived ease of use refers to the extent to which managers perceive that implementation of the machine learning system will be without unduly difficult or complicated for financial organizations (Joseph & Eaw, 2023). High perceived ease of use plays a role in the management of the attitude of managers towards the adoption of machine learning technology, particularly among decision-makers who may be placed to the position against the acceptance of technologies due to perceived complications in the implementation of the technology. The sequential technology acceptance model constructs, attitude towards use, intention to use behavior and actual system use, provides a systematic framework to understand how managers form their perspectives, adoption intentions and eventually implement machine learning technology.

In the whole of general management literature, the TAM is one of the most popular frameworks to understand the adoption of new technologies, especially in an organizational setting. TAM assumes that acceptance of a technology is primarily influenced by the ease of use and usefulness of the technology (Pajany, 2021). In the context of the project, TAM is an appropriate framework, as it can help to explain why financial managers at financial institutions in the US may or may not adopt fraud detection systems based on machine learning despite the apparent benefits of these technologies.

A very relevant secondary framework is the unified theory of acceptance and use of technology (UTAUT), which is a variation on TAM where constructs like performance expectancy, effort expectancy, social influence and facilitating conditions are included (Borhani et al., 2021). The framework that is both for scholars and practitioners makes it possible to have a nuanced understanding of the influences that impact technology adoption within organizations. In the context of the project, the addition of the additional variables will help to explain the external factors such as organisational culture, leadership support, and training which can influence a manager's decision to integrate machine learning-based fraud detection systems.

The particular problem considered under exploration is focused to know the managerial perspectives in the framework of the technology acceptance model. The research questions are designed to examine the relationship between the perceived usefulness and perceived ease of use of machine learning technology in adoption perspectives of executives, the factors that will influence the behavioral intention and what are the barriers to the actual implementation of the system. The TAM is directly aligned to the project questions by providing constructs (perceived usefulness and perceived ease of use) which can be used to explore the decision-making views of the managers towards the adoption of technology. In the current project, the TAM by Fred Davis is among the conceptual frameworks that is utilized in comprehending how the financial institution managers attitude towards a machine learning technology utilized to detect fraud is shaped and formed (Pajany, 2021). The attitude formation process is directly influenced by the basic TAM constructs (Borhani et al., 2021). The strategic thinking perspective of TAM is directly related to the results of the performance of the organization on the adoption of technology. Therefore, the framework is quite applicable to shaping thinking on management decision-making, particularly in financial services.

The TAM is based on five underlying constructs and the perceived usefulness and perceived ease of use are the keys of determining the acceptance of technology. Perceived usefulness measures people's beliefs about how a system will increase the performance of their jobs. Perceived usefulness is associated with the manner that managers and senior management come up with ideas about enhanced accuracy of fraud detection, efficiency of operations and enhancement of competitive advantage (Ayodeji, 2024). The constructs have an impact on the attitude of the users towards the technology, the intention to use the technology and the actual usage of the system. Perceived ease of use reveals the point of view of the financial managers about the openness and the ease of the implementation of the machine learning system. The constructs affect, the attitude of the user of technology, intent to use technology and finally use of the system.

With the use of TAM, the study analyzes the connection between the views of managers concerning strategic preparedness, the possibility of successful implementation of strategies, and support by organizations with the TAM constructs in situations of adoption of machine learning technology. The framework makes it easy to achieve the project objective of exploring the managerial perspectives. The framework is directly maintaining the idea of the project which aims to explore the views of the managers about the implementation of machine learning in financial institutions. The TAM is a corresponding theoretical lens of fusing the worlds of finance, technology and management, which implies that the framework is also relevant to consider in the DBA-level research that deals with understanding the processes of technology adoption decision-making.

Though the main model which is utilized in the project is the original TAM, extension of the model provides TAM that considers other variables like the 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). Similarly, the unified theory of acceptance and use of technology (UTAUT) is an amalgamation of constructs such as performance expectancy, effort expectancy, social influence, and facilitating conditions. Presumably,, the model extends to a broader range of influences on organizational and environmental factors that underlie perspectives on adoption (Zin et al., 2024). Although TAM2 and UTAUT will not be used as primary frameworks, the extended constructs from these models will inform the development of interview questions and thematic coding procedures during data analysis.

The reason that TAM is relevant in the slow machine learning technology adoption in financial institutions is that the model is able to predict key factors influencing managerial adoption perspectives and strategic alignment. Through investigating TAM elements, the project can see why some financial institutions have more favorable views about machine learning based fraud detection systems than others (Masumbuko & Phiri, 2024). The results can be directly applied to give more effective implementation strategies for machine learning based on managerial views and organisational contexts.

Within the sphere of financial services, TAM and extended constructs have been used to measure technology adoption perspectives for the effectiveness of fraud prevention. The framework is in line with the objective of the project, which is to examine the views of financial managers about the value and accessibility of machine learning in fraud prevention and operational efficiency. TAM is especially suitable for the investigation because the framework stresses the viewpoints of user acceptance, which is a critical factor in understanding the challenges of adoption of strategic machine learning initiatives in financial institutions (Rawindaran et al., 2021). Unlike technical implementation models, TAM addresses the cognitive and behavioural aspects of adoption, aligning with the project's managerial focus.

The TAM builds up a structural foundation of the literature review that provides a systematic method to organize and evaluate the research work concerning views of technology adoption in financial sectors. Thathsarani and Jianguo (2022) applied TAM theory in a qualitative study involving 487 people working in Small and Medium Enterprises (SMEs) in Sri Lanka. They found out that the digital adoption views in financial connection based on the TAM theory have a strong impact on the performances of SMEs. The scholars went further to demonstrate that financial organizations are subjected to high regulatory pressure, aggressive digital change, and growing customer security expectations, and that the latter have an effect on the way in which managers evaluate the potential of emerging technology adoption. Masumbuko and Phiri (2024) demonstrated the application of TAM and recommended the use of the framework for improving strategic management technology capability and user acceptance perspectives.

By applying TAM in fraud detection systems in financial industries, the project expands the applicability of the model into high-risk and high-compliance industries where the adoption of perspectives of AI and machine learning is both critical and complex. The work is a contribution to the literature as it serves to provide context specific information on executive perceptions and machine learning integration readiness.

Expanding TAM application from the user-level of technology acceptance to strategic managerial analysis of the technology acceptance framework to bridge the gaps between technological capability and adoption of technology decision-making frameworks. The project will provide operational strategies for fraud reduction by promoting a better matching of managerial views and the potential of technologies. The TAM will guide in the formulation of semi-structured interview questions to gather rich and qualitative responses from the financial executives on their opinions on machine learning adoption (Ebot, 2024). Questions will have probe the attitude towards the usefulness of machine learning for fraud detection, integration complexity/simplicity beliefs, and other contextual factors, such as regulatory pressure, organizational culture, leadership support for adopting the machine learning perspective etc. While there may be insights to be gained from models such as TAM2 or UTAUT to improve the analysis, the project maintains theoretical consistency by building on the original TAM framework.

During data analysis, the results obtained from financial institution manager interview will be coded using the qualitative thematic approaches. At the same time, TAM constructs will not lead to the construction of initial coding frameworks, but will be used as conceptual models for understanding emergent themes for the adoption perspectives. The project will explore recurrent features of managerial views in the use and strategic integration of machine learning systems for fraud detection (Masumbuko and Phiri, 2024). The TAM was selected because of its relevance to the opinion of technology adoption in an organizational stakeholder, particularly financial organization managers who make strategic technology decisions. Financial organizations face a set of stringent regulations, aggressive digital transformation, and increasing customer security requirements that affect how managers evaluate the potential for emerging technology adoption.

Project data may contribute to the literature in several ways. First, the data will record the views of financial managers on strategies for adopting machine learning for fraud detection and risk management. Second, the study will examine how organizational factors shape perspectives on the adoption of machine learning, including risk tolerance, regulatory compliance, technological infrastructure, and managerial readiness. Third, the project will study the correspondence between TAM constructs and real-world machine learning challenges in the context of financial fraud prevention (Gupta et al., 2025). Study data may provide lessons for how to better use machine learning as practitioners/policymakers. By investigating the intersections of technology acceptance and strategic management perspectives, the project may help close the theory-practice gap in financial management and inform improved organizational performance through more effective technology integration based on managerial 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

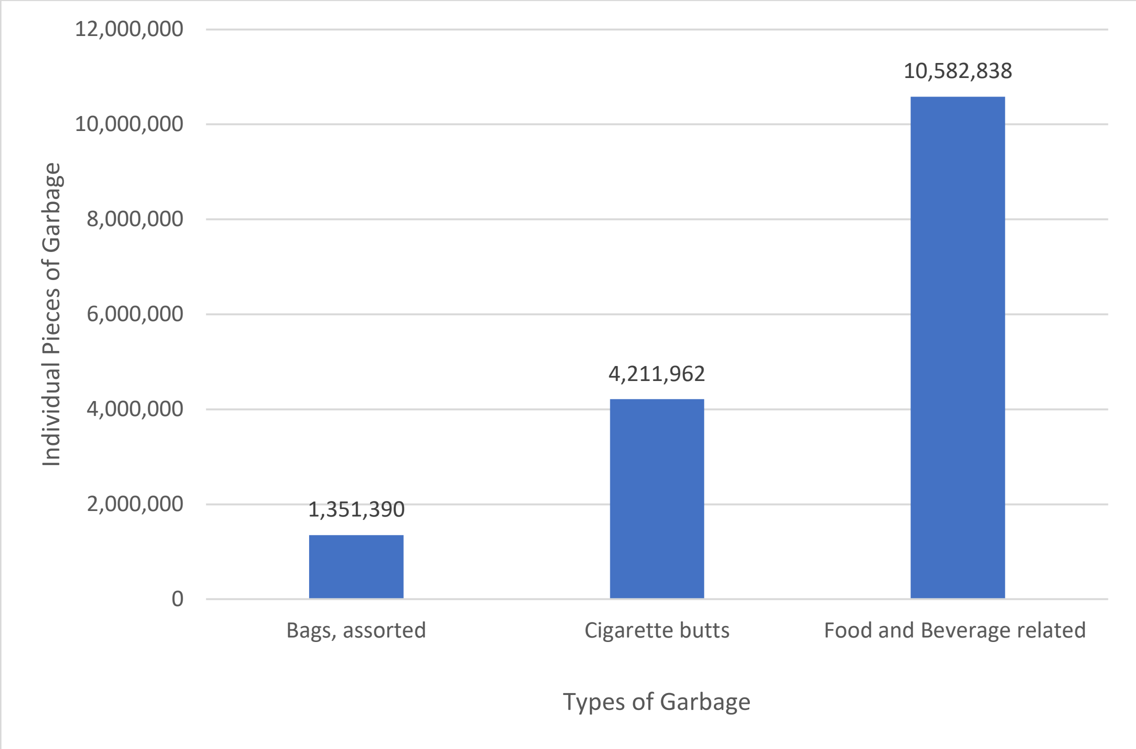
Data Collection

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 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 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 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.