The Role of AI in Fraud Detection: Are financial institutions using the most effective systems?

Hoje Jo*, Hien Bui†, and Damon Moreland‡

Abstract

This paper explores the use of AI in fraud detection and prevention, highlighting both its advantages and limitations. While AI strengthens fraud-fighting capabilities and delivers substantial cost savings, it also raises challenges related to model interpretability, ethical considerations, and regulatory compliance. System flaws can lead to severe penalties, reinforcing the need for ongoing human oversight. In this context, compliance officers, fraud analysts, and auditors remain essential for reviewing flagged anomalies, validating AI-driven decisions, and addressing complex or ambiguous cases. The study emphasizes that effective fraud prevention in the U.S. financial system requires a balanced integration of AI technologies with human judgment to ensure transparency, accountability, and compliance.

JEL CLASSIFICATION: G17, G18, K42, C53

KEYWORDS: Artificial Intelligence (AI), Fraud Detection, Fraud Prevention, Real-time Processing, Financial Institutions

I. Introduction

In this paper, the term "financial institutions" refers to entities engaged in financial and monetary transactions, such as deposits, loans, payments, and investments (Hayes et al., 2024; FinCEN, 2025). This includes traditional banks, which provide deposit-taking, lending, and investment services; credit card networks, which facilitate payment processing and authorization; and fintech companies, which deliver innovative services such as mobile banking, peer-to-peer lending, and algorithmic payments. While retailers are not classified as financial institutions under U.S. regulatory definitions, they increasingly operate as financial partners through store credit cards, installment plans, and digital wallets. Each entity contributes to the broader financial ecosystem and faces unique challenges in fraud detection and compliance. Although retailers are not formally classified as financial institutions, their role in fraud prevention has grown as point-of-sale systems now integrate real-time monitoring, encryption, and AI-based detection technologies previously reserved for banking systems (Core Payment Solutions, 2024; Georgiev, 2024). As retail transactions often initiate the fraud detection chain, their systems increasingly function as the first line of defense, particularly in card-present and card-not-present fraud scenarios. In some cases, high-volume retailers may also be subject to recordkeeping and monitoring obligations aligned with Anti-Money Laundering (AML) frameworks (Federal Deposit Insurance Corporation, 2004).

Throughout this paper, we will examine the various AI trends and advancements incorporated into financial institutions' fraud detection systems. We will also compare different AI fraud detection methodologies and discuss the ethical considerations of utilizing artificial

* Santa Clara University, hjo@scu.edu
† Santa Clara University, hbui3@scu.edu
‡ Santa Clara University, dmoreland@scu.edu

intelligence for fraud detection in financial institutions. The purpose of this paper is to outline the future of AI in combating financial fraud, suggesting the next steps for AI utilization in fraud detection systems.

The Impact of AI on Frauds and Scams

Financial fraud is an increasingly sophisticated and costly crime that often surpasses the capabilities of financial institutions and law enforcement agencies to mitigate existential threats effectively. Rapid advancements in technology have enabled nefarious criminal elements and rogue nation-states to commit crimes that are increasingly difficult to detect. As the financial market evolves with technological advancements, new financial crimes emerge alongside existing threats. For instance, financial scams, such as fake checks, ransomware, and cryptocurrency scams, have exposed new challenges that financial institutions must overcome with improved countermeasures (Reeder, 2025). Ransomware is emphasized as a significant menace, as the crime involves holding devices hostage until a ransom is paid (Reeder, 2025). Financial criminals can now inflict damage not only on consumers but also on financial institutions. Traditional fraud detection techniques, which often rely upon rule-based approaches, have been rendered useless in keeping pace with the evolving nature of financial crime. However, even with such threats in financial markets worldwide today, the rise of AI may have led to more straightforward, simpler, and more effective methods for detecting financial fraud. Unlike outdated methods used before the development of such technology, AI enables the analysis of large datasets and databases, the detection of past and present patterns, and the highlighting of anomalies in real-time. Machine Learning (ML) algorithms can now offer better protection and prevention for financial institutions against financial fraud threats. These same systems also adapt to new methods of circumventing the law, continually keeping pace with this evolving and increasingly popular threat (Kamuangu, 2024). As a result, financial institutions and government agencies have adopted advanced technologies to detect and prevent fraudulent activities. Among these new technologies, artificial intelligence (AI) has emerged as a powerful and influential tool in the fight against financial fraud. The functionality of enhancing the accuracy and efficiency of fraud detection systems offers practical solutions that counter financial criminals.

AI has played a pivotal role in modern fraud detection systems by automating threat analysis, thereby enhancing fraud prevention capabilities and reducing the need for manual intervention. Financial institutions have increasingly adopted AI technologies such as Machine Learning (ML), Deep Learning (DL), Graph Neural Networks (GNNs), and Large Language Models (LLMs) to identify and mitigate various forms of financial fraud (Flinders et al., 2025; Valleskey, 2024). These systems are deployed to combat identity theft, phishing scams, payment fraud, credit card fraud, cybercrime, and money laundering — all of which represent growing risks in digital banking environments (Butler, 2024; Flinders et al., 2025). Machine Learning (ML) algorithms are adept at analyzing historical transaction data to uncover suspicious patterns, while Deep Learning (DL) techniques detect intricate fraud schemes through their ability to learn and adapt to evolving behaviors. Graph Neural Networks (GNNs), in particular, are effective at revealing hidden relationships between entities and are valuable for analyzing complex transaction networks to expose layered fraud activity. Additionally, Large Language Models (LLMs) and Natural Language Processing (NLP) tools help extract insights from textual data, such as complaint reports or support chat transcripts, enabling banks to flag fraud signals even from unstructured sources (Valleskey, 2024; Butler, 2024).

The Improvement of Fraud Prevention and Detection Systems

Artificial intelligence (AI) offers functions and capabilities for real-time data analysis and predictive analytics, thereby enhancing automation and anomaly detection. These characteristics improve fraud prevention and detection systems from their traditional approaches. Traditional fraud detection models rely on predefined parameters, resulting in a lack of real-time and predictive analysis. Consequently, it often results in high false-positive rates and the overlooking of emerging fraud tactics. In fraud detection, real-time data analysis facilitates AI-powered systems to pinpoint and flag suspicious patterns (Valleskey, 2024). Through continuous and real-time transaction analysis, AI systems can provide immediate and direct insights into potentially fraudulent transactions. This primary function is crucial in detecting fraud promptly and preventing financial losses (Valleskey, 2024). Continuous analysis of transactions enables the prompt identification of any suspicious movements, thereby significantly enhancing the security of financial systems. Likewise, predictive analytics provides support in risk mitigation and oversight by predicting probable fraud threats through the analysis of historical and current data. Predictive models utilize historical data to identify patterns of fraudulent behavior proactively. It enhances the anticipation and certainty of possible fraud risks for detection systems. It employs techniques such as logistic regression and neural networks to make intelligent predictions about potential fraudulent activities (Valleskey, 2024). For example, AI fraud analysts can strengthen the accuracy of business risk assessments to identify high-risk customers or transactions (Valleskey, 2024). It can help fraud analysts by defining patterns and comprehending the data. This technological implementation enables financial institutions and fintech firms to employ proactive approaches, taking preventive strategies before fraud occurs, thereby reducing potential losses.

Despite these advantages, the effectiveness of AI depends on the quality of the data, model interpretability, and its integration with existing fraud detection frameworks. Human oversight remains necessary in the fraud prevention process, particularly when current technologies are not reliable against emerging threats. It highlights the need to integrate advanced technology with human supervision to combat AI-generated fraud effectively. In this context, human oversight refers to the complement of fraud investigators, compliance analysts, and internal auditors who review AI-generated alerts, make final decisions in ambiguous cases, and provide feedback loops to improve algorithmic performance. The implications of human support are required to counter new forms of AI-driven fraud, including deepfake technology. For instance, deepfake technology is a relatively new technological feature that poses new challenges to the current verification methods. Deepfake technology poses significant risks, allowing fraudsters to circumvent identity controls (Steinhaeuser, 2024). Fraudsters exploit this technology to facilitate the bypassing of KYC (Know Your Customer) identity controls used in financial institutions (Steinhaeuser, 2024). It advocates for the integration of multimodal verification methods and upgrades of detection functionalities to counter these evolving threats. The dependence solely on technology is insufficient and inadequate in the fight against AI-driven fraud (Steinhaeuser, 2024). Financial institutions, such as banks, should implement live verification steps to prevent fraudsters during the account opening process. Therefore, technology alone is insufficient in combating AI-driven fraud; thus, human oversight is crucial.

In addition to ensuring operational effectiveness, human oversight plays a strategic role in maintaining accountability, fairness, and ethical compliance in AI-driven fraud detection systems.

Oversight is not merely reactive, but a critical mechanism for aligning AI decision-making with institutional values and regulatory mandates (Lumenova AI, 2024). Human reviewers can identify model drift, intervene in ambiguous cases, and interpret anomalies in ways that automated systems cannot (Rodgers et al., 2023). Furthermore, oversight is essential in enforcing transparency and explainability, both of which are increasingly demanded by financial regulators and stakeholders (Cornerstone, 2025). Without this layer of governance, institutions risk deploying black-box models that may be technically sound but ethically or legally flawed. As financial institutions adopt more advanced AI systems, embedding structured oversight becomes not just a safeguard but a strategic necessity.

Advanced Applications of AI in Fraud Detection: CNNs and Blockchain Integration

Recent advancements in AI have introduced novel methodologies for fraud detection, particularly through the integration of Convolutional Neural Networks (CNNs) and blockchain technology. These technologies offer complementary strengths that enhance the robustness and transparency of fraud detection systems. CNNs, traditionally used in image and pattern recognition, are increasingly being applied to financial fraud detection, especially in analyzing smart contracts and transactional documents. According to Louati et al. (2024), CNNs can be trained on datasets containing both legitimate and fraudulent smart contracts to identify subtle patterns indicative of fraud. This approach enables the detection of anomalies in both textual and transactional data, offering a powerful tool for legal and financial compliance. CNNs also show promise in document verification, where they can analyze scanned documents or digital forms for signs of tampering or forgery. Their ability to process high-dimensional data makes them suitable for identifying complex fraud schemes that traditional models might overlook.

Blockchain technology, with its decentralized and tamper-resistant ledger, provides a secure foundation for storing and verifying transaction data. When combined with AI, particularly machine learning and deep learning models, blockchain can significantly enhance fraud detection capabilities. Ketha and Provodnikova (2024) propose a framework where AI algorithms analyze blockchain transaction patterns to detect anomalies in real-time. This integration ensures that once fraudulent behavior is detected, the associated data cannot be altered, thereby preserving the integrity of the evidence. Moreover, blockchain can support smart contract auditing, where AI models continuously monitor contract execution for deviations from expected behavior. This is particularly useful in decentralized finance (DeFi) platforms, where traditional oversight mechanisms are limited.

AI Implications of Fraud Prevention and Detection Systems in Different Industries

One of the benefits of AI implications is the decrease in credit card fraud. The rise of alternative payment methods, including digital wallets and P2P (peer-to-peer) payments, reflects varying consumer preferences and showcases the industry's adaptation to consumers' demands. Artificial intelligence (AI) is considered a favorable resolution to fight A2A (Account-to-Account) fraud risks. The primary risk in account-to-account transactions is social engineering scams, with 65% of respondents being optimistic about AI's effectiveness (MasterCard, 2024). Visa and Mastercard utilize Machine Learning (ML) models to examine real-time transaction patterns, which significantly lessens the incidence of fraudulent activities (Fitzpatrick, 2024). As elaborated, Visa utilizes advanced analytics to detect and note suspicious transactions, resulting in enhanced

security for cardholders. A survey indicates that 63% of respondents prioritize advanced fraud detection as a driver for AI investment (MasterCard, 2024). By cultivating the functionalities of Machine Learning (ML), these systems can analyze vast amounts of transaction data. AI helps identify and prevent fraudulent activities before they escalate. 49% of financial institutions and fintech firms have already integrated AI, while 93% plan to invest and implant AI within the next 2-5 years (MasterCard, 2024). These statistics further underscore the growing confidence in digital transactions and overall financial security. It indicates a notable shift in the perception of technology for fraud prevention and detection systems. The convergence of AI with traditional systems streamlines workflows in detecting and preventing fraud. Across the board, AI's proficiency in adapting to new fraud movements guarantees that detection systems remain effective against emerging threats within financial institutions.

As a result of advanced AI implementation, fraud detection systems in retail have become more sophisticated, ensuring a secure environment for all stakeholders, including businesses and customers. There is a growing collaborative dynamic between retailers and financial institutions, in which data and feedback are shared to continuously improve fraud prevention efforts across the transaction chain. In a typical retail transaction, fraud detection begins at the point of sale, where retailers use AI-powered POS systems equipped with encryption, tokenization, and real-time screening tools to flag suspicious activity (Core Payment Solutions, 2024). These transactions are then routed through credit card networks such as Visa or Mastercard, which apply their own fraud scoring algorithms based on spending patterns and geolocation. Finally, issuing banks, which fund the transactions, apply backend AI models to detect anomalies, evaluate risk, and flag chargebacks or fraudulent claims. At each stage, distinct AI systems operate independently but contribute to shared fraud intelligence platforms, facilitating collaborative risk reduction across the ecosystem (Georgiev, 2024). In some cases, retailers also face compliance expectations related to fraud prevention and may be required to maintain transaction records or adhere to data standards, particularly when working with regulated financial intermediaries (Federal Deposit Insurance Corporation, 2004).

Typical retail fraud types are credit card fraud and account takeover (Pavion, 2024). These threats necessitate the need for advanced detection systems. Retail businesses utilize AI to implement sophisticated algorithms that pinpoint and mitigate fraudulent activities in real-time (Pavion, 2024). AI plays a significant role in protecting assets and customers from fraudulent activities for retail businesses. Financial frauds cause immediate financial losses and additional costs for investigation and recuperation. Customers' faith and belief are adversely impacted by fraud, which subsequently affects potential long-term business growth results. AI systems utilize predictive analytics to forecast potential fraudulent activities, providing retailers with real-time alerts (Pavion, 2024). Automation of fraud investigation approaches through AI provides valuable insights for informed decision-making (Pavion, 2024). The role of AI is pivotal in ensuring a secure retail environment amidst growing challenges. It further improves retail businesses' ability to safeguard assets and customer trust. The integration of AI and predictive analytics lets retailers forecast and prevent fraudulent activities effectively (Pavion, 2024). Overall, the continuing advancement of technology will further empower AI in combating fraud in retail environments. These interconnected systems underscore the importance of continuous feedback and cooperation across the transaction chain, enabling AI models to evolve in response to emerging fraud patterns. It highlights how collaboration between retailers, credit card networks, and financial institutions is essential to building resilient and adaptive AI fraud detection systems.

Regulatory and Compliance Implications of AI Systems

As AI can enhance fraud detection, it unfortunately can enable sophisticated scams and frauds (West and Ciais, 2023). Cooperation across financial sectors is integral to developing safeguards against AI-enabled fraud. The need for protective and defensive measures against AI misuse must be emphasized. AI presents significant risks and opportunities in tackling financial fraud and scams. The challenge necessitates protective standards and benchmarks that do not hinder innovation. AI implications can enhance fraud detection, enabling banks to identify fraud more effectively while also facilitating the detection of unlawful activities (West and Ciais, 2023). Collaboration across sectors is crucial for achieving long-term reductions in fraud and scams. As AI implementation also has adverse impacts, it presents new challenges for financial institutions, such as ethical considerations and regulatory compliance, which must be addressed to ensure the effective and responsible use of AI technologies. Organizations with ineffective fraud prevention and detection systems are vulnerable to severe financial obligations and penalties imposed by various regulations and agencies.

One of the regulations that financial institutions typically encounter is the Anti-Money Laundering (AML) regulations. Financial institutions must adhere to AML (Anti-Money Laundering) regulations to ensure compliance with international frameworks for preventing financial crime (Crane and Kimbrell, 2025). AI-driven fraud detection systems are increasingly being incorporated into AML compliance programs. The purpose of the integration is to strengthen transaction monitoring, recognize suspicious movement, and enhance reporting efficiency (Crane and Kimbrell, 2025). AI algorithms can detect complex money laundering patterns that traditional rule-based systems might neglect, which reduces false positives while improving accuracy (Crane and Kimbrell, 2025). Nevertheless, significant challenges remain in aligning AI fraud detection models with AML regulations. Financial institutions faced nearly $5 billion in fines for AML and KYC failures in 2022 (Levitt, 2024). Financial institutions must further utilize Deep Learning (DL) and Natural Language Processing (NLP) to enhance identity verification for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance (Levitt, 2024). The regulation requires financial institutions to demonstrate transparency and accountability in their anti-money laundering (AML) compliance strategies. AI models must ensure explainability and fairness in decision-making processes to meet compliance requirements (Crane and Kimbrell, 2025). Furthermore, cooperation among financial institutions, regulatory agencies, and AI developers is necessary to establish standardized AI governance frameworks that strike a balance between technological advancements and compliance requirements.

While this section references select foreign regulatory bodies, the primary regulatory framework examined throughout this paper is that of the United States. The inclusion of international examples, such as the European Union or Singapore, serves only to provide comparative context and highlight alternative approaches to AI governance. Many AML violations stem from inadequate monitoring systems. AI-powered fraud detection, when properly implemented, can enhance transaction monitoring and reduce false negatives, thereby helping institutions meet AML compliance standards. As different financial institutions are based in various countries, it is mandatory to comply with the standards and regulations of the governing agencies in each respective country. The U.S. approach to governing AI relies on existing regulatory frameworks rather than designing comprehensive new legislation. The enforcement of AI governance in the United States is handled by established agencies, including the U.S. regulatory agencies (Simpson, 2023). The U.S. government intends to utilize existing regulatory

agencies to oversee the deployment of AI and refine existing regulations. Unlike other regions, the U.S. does not have a comprehensive AI legislation framework in place (Simpson, 2023). The implication of that means that the governance of AI is more fragmented and relies heavily on the interpretation and application of existing laws by these agencies. Each agency is taking specific actions to address AI-related issues. For example, the CFPB has administered guidance demanding that creditors use algorithms to provide transparent reasons for adverse credit decisions, ensuring clarity in automated decision-making (Simpson, 2023). On the contrary, the European Union's Artificial Intelligence Act was published in the EU Official Journal, marking it as the first comprehensive horizontal legal framework for regulating AI systems across the EU, on 12 July 2024 (Hickman et al., 2024). The EU is implementing the EU AI Act through a rigorous process involving multiple stakeholders to ensure seamless integration of the legislation. An AI Board will be appointed to supervise the enforcement of the law across member states, while the details of enforcement at the national level are still under discussion. There is a current debate about whether a centralized regulatory body would be sufficient to guarantee consistent enforcement of AI regulation. The EU approach focuses on ethics, emphasizing compliance, accountability, and the ethical use of AI technologies.

The role of internal audit

As AI becomes more embedded in financial fraud detection systems, the role of internal audit has expanded from retrospective reviews to a strategic function that proactively assesses AI-related risks and controls. Internal auditors are now tasked with evaluating the integrity and transparency of AI models, ensuring that fraud detection systems are not only effective but also compliant with emerging regulatory and ethical standards (CSM & CO LLP, 2025). In high-risk environments, internal audit helps identify weaknesses in model governance, bias detection, data management, and system accountability. Moreover, audit teams have begun leveraging AI tools themselves—using anomaly detection, continuous monitoring, and predictive analytics to simulate fraud scenarios and uncover operational blind spots (Hodge, 2024). This transformation positions internal audit as a vital bridge between compliance, cybersecurity, and business operations. Beyond technical assessments, internal auditors also help cultivate a culture of fraud awareness by advising management, training employees, and validating the effectiveness of human oversight protocols (Petrașcu & Tieanu, 2014). As financial institutions face increasingly complex threats from AI-enabled fraud, the internal audit function will play a central role in reinforcing trust, transparency, and institutional resilience.

As AI systems become more autonomous and complex, internal audit functions are increasingly expected to provide assurance not only over outcomes but also over the processes and algorithms that drive decision-making. This includes validating data inputs, assessing model training practices, and ensuring that AI deployment aligns with institutional policies and regulatory expectations (CSM & CO LLP, 2025). Internal auditors must now work closely with data scientists, compliance officers, and IT security teams to evaluate how fraud detection models are governed, monitored, and updated over time. The rapid pace of AI innovation also introduces the risk of model drift, which internal audit can help detect through independent testing and validation processes. According to Hodge (2024), internal auditors must adopt a forward-looking mindset that anticipates how fraudsters may exploit AI vulnerabilities, including adversarial attacks and synthetic identity generation. Additionally, by integrating ethics-based auditing techniques, internal audit can help ensure AI decisions reflect principles of fairness, accountability, and

transparency—especially as regulators intensify their scrutiny of algorithmic systems (Petrașcu & Tieanu, 2014). This expanded scope repositions internal audit as not just a control mechanism but a strategic partner in sustaining the integrity and trustworthiness of AI-driven fraud prevention.

Thesis Statement

Overall, the incorporation of AI in fraud detection presents several challenges. Issues such as model interpretability, ethical considerations, and regulatory compliance must be addressed to ensure the effective and responsible use of AI technologies. As financial institutions increasingly adopt AI-powered fraud detection systems, their effectiveness varies depending on the models used, such as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP), as well as compliance with evolving regulatory standards. While AI has significantly improved the accuracy and response speed of fraud detection, challenges such as false positives, algorithmic bias, and regulatory scrutiny raise concerns about whether financial institutions are leveraging the most effective systems for fraud prevention. This paper aims to examine the strengths and limitations of AI fraud detection models and highlight the need for optimized, transparent, and compliant AI-driven solutions. To guide this analysis, the paper proposes a conceptual model that maps how AI systems interact with institutional capabilities, regulatory constraints, and operational outcomes in fraud detection. This model serves as a structural lens for evaluating which AI approaches are most effective, under what conditions, and why some are more widely adopted despite technical trade-offs. The scope of this paper is to study the implications of financial institutions and regulatory frameworks in the United States. References to non-U.S. jurisdictions, such as the European Union, are included for comparative analysis and evaluation purposes. By examining these features, this paper will highlight the need for optimized, transparent, and compliant AI-driven solutions to safeguard financial systems and counter increasingly sophisticated fraud threats. As this paper aims to contribute to and shape the future of AI in addressing financial fraud, the need for optimized and compliant AI-driven solutions will strongly emphasize the next step in AI integration for fraud detection systems.

II. Literature Review

The growing integration of AI-powered fraud prevention and detection systems has led to an increasing number of studies analyzing their effectiveness, benefits, and challenges. Multiple research papers have explored different AI techniques in fraud detection and prevention. Several studies also highlight AI's ability to improve accuracy, enhance real-time monitoring, and reduce false positives. Other studies have examined the challenges associated with data quality, algorithm bias, and regulatory compliance for practical implementation in banking and financial institutions. This section reviews key studies in the field and provides an overall understanding of AI-driven fraud detection.

AI-Driven Fraud Detection in Financial Institutions

Several studies have evaluated the role of AI in fraud detection within the banking sector, analyzing AI and data science techniques for banking fraud detection and highlighting cybersecurity improvements (Olowu et al., 2024). The paper, "AI-Driven Fraud Detection in Banking: A Systematic Review," examines AI and data science techniques for fraud detection in

the banking sector. It highlights the need for advanced detection strategies in response to the growing financial fraud and cybersecurity threats. The study finds that Machine Learning (ML) algorithms achieve fraud detection rates between 87% and 94%, concurrently reducing false positives by 40% to 60% compared to traditional methods (Olowu et al., 2024). The study further recommended the development of explainable AI frameworks to provide transparency and rationale for the decision-making process. The research also suggests hybrid detection systems that combine multiple AI technologies to enhance fraud detection capabilities (Olowu et al., 2024). Additionally, the review highlights the importance of regulatory compliance and legal considerations when implementing AI in fraud detection.

Olowu and Adeleye (2024) conducted a systematic review of AI techniques in banking fraud detection, reporting that ML algorithms achieved detection rates between 87% and 94% while reducing false positives by up to 60%. While these results underscore the efficiency of ML in identifying fraudulent patterns, the study does not address the interpretability of these models, an essential factor for regulatory compliance. Moreover, the exclusive focus on ML overlooks the potential benefits of hybrid systems, as emphasized by Yuhertiana and Amin (2024). Thus, while Olowu and Adeleye's findings support the integration of AI in fraud detection, they also reveal gaps that must be addressed to ensure robust, transparent, and compliant systems.

Furthermore, there are papers and studies on the review of AI methodologies and driven approaches for financial fraud detection (Yuhertiana and Amin, 2024). The paper "Artificial Intelligence Driven Approaches for Financial Fraud Detection: A Systematic Literature Review" presents a systematic literature review on AI methodologies for detecting financial fraud. A systematic literature review was conducted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) approach. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) is a set of guidelines that help authors report systematic reviews and meta-analyses. As a result, the paper acknowledges the effectiveness of AI in enhancing the precision and efficiency of fraud detection. The financial industry is highlighted as the primary sector for AI applications in fraud detection (Yuhertiana and Amin, 2024). Artificial intelligence plays a pivotal role in identifying anomalies in financial transactions, which is crucial for security. Machine Learning (ML) models and techniques remain the prevailing methodology in financial fraud detection (Yuhertiana and Amin, 2024). The study analyzes and examines 24 papers published between 2014 and 2023 (Yuhertiana and Amin, 2024). The paper concludes that AI dramatically improves the precision and efficiency of fraud pattern identification in the financial industry. It further emphasized that AI simulates human cognitive abilities within a machine framework (Yuhertiana and Amin, 2024). AI's effectiveness mostly depends on acquiring experience and data for optimal performance. AI has the ability to learn from experiential data without explicit human guidance autonomously.

AI-Based Fraud Detection Systems

Furthermore, there are papers that provide a review of various AI-based methods, including machine learning (ML) and deep learning (DL) algorithms, used for detecting credit card fraud (Hafez et al., 2025). One popularly implemented approach is Machine Learning-Based fraud detection, which utilizes both supervised and unsupervised learning methods to identify fraudulent activities. Supervised learning algorithms are employed as the primary tools in financial fraud detection, where historical transaction data serves as a reference (Kamuangu, 2024). Each instance in the dataset is labeled as either fraudulent or non-fraudulent, allowing the system algorithms to

learn from these examples and generalize to new, unseen transactions. Supervised learning models, such as decision trees and logistic regression, are trained on labeled datasets of fraudulent transactions, enabling them to classify future transactions with high accuracy (Kamuangu, 2024). Unsupervised learning techniques, including clustering and anomaly detection algorithms, facilitate the identification of unknown fraud patterns that were not previously present in historical datasets (Hafez et al., 2025). Unsupervised learning is crucial in navigating the complexities of financial data, where fraudulent activities are often rare and hidden within vast datasets. These techniques, such as clustering algorithms like K-Means, are particularly useful at identifying unusual patterns and transactions that deviate from regular patterns (Kamuangu, 2024). The study evaluates and compares these techniques to identify their strengths and weaknesses. The author summarizes the major challenges, including data imbalance and high processing demands, faced by current AI models used in fraud detection. The author even advocates for the implementation of hybrid and ensemble models that combine machine learning (ML), deep learning (DL), and multi-objective heuristic optimization (MHO) techniques, which could enhance detection accuracy and address class imbalance (Hafez et al., 2025).

AI-based fraud detection systems use advanced Machine Learning and Neural Network models to enhance the accuracy and speed of identifying fraudulent transactions. These systems surpass traditional rule-based methods due to their ability to detect evolving fraud patterns. Several papers have examined the benefits of utilizing AI over traditional rule-based systems. The paper by Cheemakurth et al. (2024) explains how neural network models can enhance financial security by enabling the highly accurate and rapid detection of fraudulent transactions in real-time. It is emphasized that AI reduces false positives, improving operational efficiency and minimizing disruptions to legitimate transactions. The study yielded a finding that Neural Network methods outperformed traditional Machine Learning methods, achieving a fraud detection accuracy of 98% (Cheemakurth et al., 2024). The author further explains how Neural Network models surpass traditional methods due to the model's adaptability to evolving fraud patterns and ability to identify new fraudulent activity.

Regulatory Challenges and Ethical Considerations

Despite the benefits that AI brings to fraud detection, the technology faces several challenges, including model interpretability, ethical considerations, and regulatory compliance. Understanding how AI models arrive at their conclusions can be challenging, making it difficult to explain fraud detection decisions. Ethical concerns regarding privacy and potential bias in AI algorithms when analyzing personal data should also be addressed. "The paper by Adhikari et al. (2024) outlines how AI enhances real-time fraud detection, adaptability, and scalability compared to traditional systems. The study also explains how AI systems outperform traditional rule-based systems, particularly in real-time detection and adaptation, enabling the detection of evolving fraud patterns. The study's findings indicated that AI significantly enhances fraud detection accuracy but also presents challenges related to ethical concerns, algorithmic bias, and data privacy (Adhikari et al., 2024). The research highlighted the need for high-quality data to improve AI performance and acknowledged the vulnerabilities of AI systems to adversarial attacks. The research highlights the importance of high-quality data in enhancing AI performance and acknowledges the vulnerabilities of AI systems to adversarial attacks. The study concluded that while AI-based fraud detection outperforms rule-based methods, addressing bias and ensuring data security remain critical challenges (Adhikari et al., 2024). The study concurs with the notion that while AI-based fraud

detection outperforms rule-based methods, addressing bias and ensuring data security remain critical challenges.

Addressing regulatory and legal challenges is vital for the effective deployment of AI fraud detection systems. Since the EU governing bodies have comprehensive AI regulations in place, there is a well-defined range of penalties for defective and ineffective AI systems. For example, the maximum penalty for providing incorrect, incomplete, or misleading information to notified bodies or national competent authorities is EUR 7.5 million or 1 percent of the worldwide annual turnover, whichever is higher (Hickman et al., 2024). Financial institutions need to carefully develop AI systems to ensure their effectiveness when deploying them in EU territories. In the United States, financial institutions are required to comply with regulations established by the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB). It highlights the various approaches to AI regulatory enforcement worldwide. It further emphasizes the importance of developing robust regulatory frameworks that strike a balance between innovation and the protection of fundamental human rights and safety.

The literature increasingly highlights the essential role of human oversight in ensuring ethical and effective deployment of AI technologies, particularly in domains involving high-stakes decision-making such as fraud detection. Petrașcu and Tieanu (2014) argue that internal audit is not merely a control mechanism but a value-adding function that supports leadership in managing fraud risks, offering both preventive and detective insights that are vital in technologically complex environments. As AI-driven systems grow more autonomous and opaque, ethical risks emerge around bias, explainability, and accountability—challenges that cannot be addressed through automation alone. Rodgers et al. (2023) reinforce this view by proposing an ethical decision-making framework—the Throughput Model—that maps how perception, judgment, and choice shape algorithmic decisions. Applied to AI governance, this model underlines the importance of embedding human evaluators, such as internal auditors, into algorithmic systems to oversee input quality, decision logic, and outcome integrity. Together, these perspectives support a growing consensus that internal audit functions are indispensable not just for verifying technical compliance but for upholding organizational integrity and ethical accountability in the age of AI.

III. Evaluating the Effectiveness of AI-Powered Fraud Detection in Financial Institutions

This section provides a qualitative literature synthesis and secondary data analysis approach to evaluate the effectiveness of AI-powered fraud detection systems in financial institutions. This methodology is appropriate for two reasons. First, the deployment of AI in fraud detection is a relatively recent and fast-evolving area, with limited access to standardized empirical datasets. Second, regulatory bodies, industry leaders, and financial institutions have released a growing volume of publicly available reports, case studies, and enforcement actions that offer credible, real-world insights into AI's current capabilities and limitations. By synthesizing these sources, this section aims to map where AI is most effective, assess the performance trade-offs among model types (e.g., Machine Learning, Deep Learning, Natural Language Processing), and evaluate how institutional failures, despite AI adoption, continue to result in regulatory penalties and financial harm. The sources used in this section were selected based on recency (2022–2025), relevance to AI fraud detection, and institutional credibility, such as peer-reviewed studies, regulatory reports, and widely cited industry white papers. This ensures that the comparative evaluations and enforcement case analysis reflect current and authoritative perspectives.

To evaluate the effectiveness of AI-powered fraud detection systems, this section presents a three-part framework: (1) a conceptual model illustrating institutional touchpoints for AI intervention; (2) a comparative analysis of common AI model types used in fraud detection; and (3) real-world evidence from enforcement actions that reveal where failures persist despite AI deployment. Together, these components provide a holistic view of AI's promise, limitations, and institutional fit.

Simple Model for AI's Impact on Fraud Detection in Financial Institutions

Key Variables

- Input Variables (X):
  - Transaction Volume (V): Number of transactions processed per day.
  - Fraud Rate (F): Percentage of fraudulent transactions before AI implementation.
  - AI Detection Accuracy (A): AI's ability to correctly identify fraud (True Positive Rate).
  - AI False Positive Rate (FP): AI incorrectly flags legitimate transactions as fraud.
  - Manual Review Cost (C): Cost per transaction for human review.
  - Fraud Loss per Incident (L): Average loss per undetected fraudulent transaction.
- Output Variables (Y):
  - Reduction in Fraud Loss (ΔL): Savings from AI detecting more fraud.
  - Operational Cost Savings (ΔO): Savings from reduced manual reviews.
  - False Positive Cost (CFP): Additional cost from AI's false alarms.

Model Equations

(A) Fraud Detection Improvement

- Fraud Detected by AI (DF):
  $DF = V \times F \times ADF = V \times F \times A$
- Reduction in Fraud Loss (ΔL):
  $\Delta L = DF \times L\Delta L = DF \times L$

(B) Operational Efficiency

- Reduction in Manual Reviews (ΔR):
  $\Delta R = V \times F \times (1 - Aprior - A)\Delta R = V \times F \times (1 - Aprior - A)$
  (where AprioriAprior is pre-AI detection rate)
- Operational Cost Savings (ΔO):
  $\Delta O = \Delta R \times C\Delta O = \Delta R \times C$

(C) False Positive Cost

- False Positives Flagged (FP_T):
  $FPT = V \times (1 - F) \times FPFPT = V \times (1 - F) \times FP$
- Cost of False Positives (CFP):
  $CFP = FPT \times CCFP = FPT \times C$

Net Impact of AI on Fraud Detection

Net Impact $= \Delta L + \Delta O - CFP$Net Impact $= \Delta L + \Delta O - CFP$

Example Calculation

Assume:

- V = 10,000V = 10,000 transactions/day
- F = 1%F = 1% fraud rate
- A = 95% A = 95% detection accuracy
- FP = 2%FP = 2% false positive rate
- C = $5C = $5 per manual review
- L = $500L = $500 per fraud

Calculations

(A) Fraud Detected by AI:

DF = 10,000×0.01×0.95 = 95 frauds caught = 10,000×0.01×0.95 = 95 frauds caughtΔL = 95×500 = $47,500 savedΔL = 95×500 = $47,500 saved

(B) Operational Savings (assuming prior detection = 80%):

ΔR = 10,000×0.01×(1−0.80−0.95) = N/A (adjust based on actual workflow)ΔR = 10,000×0.01×(1−0.80−0.95) = N/A (adjust based on actual workflow)

(Simpler alternative: AI reduces manual reviews by 50%)

ΔO = 5,000×5 = $25,000 saved ΔO = 5,000×5 = $25,000 saved

(C) False Positive Cost:

FPT = 10,000×0.99×0.02 = 198 false alarmsFPT = 10,000×0.99×0.02 = 198 false alarmsCFP = 198×5 = $990CFP = 198×5 = $990

(D) Net Impact:

$47,500+$25,000−$990 = $71,510 net benefit/day$47,500+$25,000−$990 = $71,510 net benefit/day

Limitations & Considerations

- AI Model Drift: Fraud patterns evolve; AI needs retraining.
- Customer Experience: High false positives may frustrate users.
- Integration Costs: The initial setup and maintenance costs for AI are not included in the price.

To quantify the operational impact of AI on fraud detection, a hypothetical scenario was applied using the conceptual model. With a detection accuracy of 95%, a false positive rate of 2%, and 10,000 daily transactions, the institution would save approximately $47,500/day in fraud losses and $25,000/day in reduced manual reviews, incurring only $990 in false positive costs, yielding a net benefit of $71,510 per day, or nearly $18 million annually. This calculation, while simplified, underscores the substantial cost-saving potential of AI tools under high-performance conditions. These savings assume high model performance with levels that align most closely with advanced supervised machine learning (ML) or deep learning (DL) systems, both of which have been widely adopted across financial institutions. The next section compares these AI models across key operational criteria to evaluate their real-world effectiveness.

This simple model helps quantify the impact of AI on fraud detection in financial institutions. We can adjust variables based on real-world data for accuracy. While the conceptual model maps out where AI tools are deployed across institutions, the next section examines the relative strengths and weaknesses of specific AI model types used at those intervention points. Based on research and reviews, it is apparent that Machine Learning techniques have been extensively used to enhance fraud detection and prevention systems compared to other methods.

Studies have shown that the integration of AI has significantly improved the preventive and defensive strategies of financial institutions. To gain additional insights, this paper aims to explore the adoption of AI techniques and models within fraud detection and prevention systems. The study will utilize available data and statistics to validate the current understanding of AI implementation and effectiveness in financial institutions. One of the objectives is to identify the most effective AI models and techniques. The purpose of this study is to suggest a suitable AI model for financial institutions to implement, ensuring compliance with regulations and legislation. Subsequently, it can provide a material and significant net benefit to the fraud detection system.

Comparative Data and Performance Metrics

Performance Across Different AI Models

The BioCatch 2024 AI Fraud Financial Crime Survey provides critical empirical support for the findings presented in this paper. As one of the most comprehensive industry surveys on AI adoption in fraud detection, it offers valuable context for interpreting the performance metrics of AI models discussed earlier.

According to the survey, 94% of financial institutions report using AI/ML techniques to assess risk from user behavior, and 87% state that AI has improved the speed of fraud detection. These figures reinforce the high adoption rate of Machine Learning (ML) models (Table 2) and validate their perceived effectiveness in real-world applications. Furthermore, the survey reveals that 73% of firms use AI specifically for fraud detection, underscoring the centrality of AI in modern fraud prevention strategies.

Importantly, the BioCatch survey also highlights the evolving threat landscape. For example, 91% of banks reconsidered voice verification methods due to the rise of AI-enabled fraud, such as deepfake audio attacks. This finding supports the paper's broader argument that AI systems must be continuously updated and supplemented with human oversight and explainable AI frameworks to remain effective.

Regulatory & Compliance Challenges for AI Fraud Detection

Despite the advantages of AI-powered fraud detection systems, financial institutions constantly face regulatory scrutiny and compliance challenges. Most compliance shortcomings and violations are related to AML compliance. While the U.S. has implemented robust AML regulations through agencies such as FinCEN (Financial Crimes Enforcement Network) and the OCC (Office of the Comptroller of the Currency), similar regulatory frameworks in the European Union, such as the 6th AML Directive, offer useful points of comparison, particularly in areas like data sharing and enforcement structure. Although the primary focus remains on U.S. regulatory practices and institutional frameworks, brief references to international standards, such as the EU's AML requirements, are included to contextualize broader trends in AI compliance. References to European directives serve to highlight cross-jurisdictional trends in AI-driven fraud prevention. Key concerns include (BioCatch, 2024):

- 51% of financial institutions and fintech firms lost between $5 million and $25 million to AI-driven threats in 2023.
- 91% of banks reconsidered voice verification methods due to AI-enabled fraud risks.

- Fines for Anti-Money Laundering (AML) violations surged by 50% in 2022, totaling nearly $5 billion.
- Notable cases include:
    - 2022:
        - Morgan Stanley was fined $60 million to resolve a data security lawsuit (Stempel, 2022).
        - Global AML Fines (Various Banks) totaled $5.0 billion (BioCatch, 2024).
    - 2023:
        - Deutsche Bank fined $186 million for AML shortcomings (BioCatch, 2024).
        - Binance faced a $4.3 billion penalty for AML violations (BioCatch, 2024).
    - 2024:
        - Toronto-Dominion Bank (TD Bank) faced a $3.0 billion fine for AML violations (Emanuel-Burns, 2024).
        - City National Bank was fined $65 million to resolve risk control allegations (ABA Banking Journal, 2024).
    - 2025:
        - Paypal was fined a $2 million civil fine over cybersecurity failures that led to the exposure of customers' Social Security numbers (Stempel, 2025).
        - OKX agreed to pay penalties of more than $500 million for violating U.S. Anti-Money Laundering Laws (United States Department of Justice, 2025).

Research Methodology

Performance Across Different AI Models

To understand the complete perspective of AI fraud detection's effectiveness, the paper aims to compare and examine the following models and techniques used by financial institutions:

- Machine Learning (ML)-based models
- Deep Learning (DL) techniques
- Natural Language Processing (NLP)

To assess the effectiveness of AI-powered fraud detection systems in financial institutions, the paper will use qualitative metrics for measuring success. The rating will be determined based on a combination of industry reports and academic research. The following key comparison metrics are used to gain more detailed and precise insights:

- False positive rates: aim to measure the frequency of legitimate transactions being flagged as fraud.
    - Low: Less than 1% of legitimate transactions incorrectly flagged; indicates strong precision and minimal manual review burden (BioCatch, 2024; Adhikari et al., 2024).
    - Medium: 1%–3% false positive rate; manageable in large institutions with tiered fraud review protocols.
    - High: Greater than 3% of legitimate transactions flagged as fraud; often results in customer dissatisfaction, increased operational costs, and elevated risk of revenue loss due to false declines (Levitt, 2024; Bengani, 2024).

- Detection speed: aims to determine how quickly AI models identify fraudulent activity.
    - Very Fast: Response time ≤ 100 milliseconds; latency optimized through real-time inference pipelines using high-performance hardware and minimal preprocessing (Cheemakurthi et al., 2023; NVIDIA, 2024).
    - Fast: Response time between 100–500 milliseconds; typical of optimized ML pipelines with efficient data ingestion and model simplicity (Levitt, 2024).
    - Medium: Response time between 500 milliseconds and 1 second; often associated with NLP or multi-layered fraud scoring systems requiring contextual validation.
    - Low: Response time ≥ 1 second; typically seen in models that require external data sourcing, intensive feature extraction, or human-in-the-loop validation prior to flagging a transaction (BioCatch, 2024; Adhikari et al., 2024).
- Industry Effectiveness Rating
    - Derived from a combination of adoption rates, reported detection performance in financial institutions, and model preference trends highlighted in BioCatch (2024) and Bengani (2024). "Very High" implies consistent preference by top-tier banks due to accuracy and integration success; "Medium" indicates moderate adoption or use for niche tasks like NLP-based anomaly descriptions.

The data and examples cited in this section were selected based on three key criteria: (1) recency — sources published between 2022 and 2025 to reflect the most current developments in AI-based fraud detection; (2) credibility — reports and findings issued by reputable institutions such as BioCatch, industry surveys, and major regulatory bodies; and (3) relevance — sources that directly address the technical performance or compliance challenges of AI-powered fraud detection in financial institutions. For the comparative evaluation of AI model performance (e.g., ML, DL, NLP), the analysis draws primarily from BioCatch's 2024 industry report, which provides adoption rates and qualitative performance ratings.

Regulatory & Compliance Challenges

A secondary analysis examines the compliance of AI fraud detection with financial regulations (e.g., GDPR, EU AI Act, AML laws). The purpose of this research is to determine whether financial institutions are effectively implementing their AI-powered fraud detection systems. The extent and materiality of fines and penalties can illustrate the severity of system deficiencies and flaws. Key areas of this secondary analysis include:

- Case studies of legal challenges related to AI-driven fraud detection failures.
- Comparison Metrics:
    - Fines issued for AI compliance failures (monetary penalties imposed on financial institutions)
    - Regulatory Violations (reasons and rationale for fines and penalties)

For the enforcement case analysis, multiple sources were used, including official regulatory filings, news reports (e.g., Reuters, Bloomberg), and government publications (e.g., DOJ press releases), to provide a comprehensive view of where AI deployment has failed to prevent compliance breaches or mitigate risk exposure.

Key Findings and Institutional Implications

The expectations outlined in this section are grounded in both empirical insights and evolving industry standards. Studies have shown that Deep Learning (DL) models outperform traditional Machine Learning (ML) models in identifying complex fraud patterns due to their capacity to process vast and unstructured datasets efficiently (Adhikari et al., 2024; Hafez et al., 2025). However, Machine Learning (ML) remains favored in practical settings for its interpretability, lower computational cost, and ease of integration—critical attributes for regulatory compliance and operational scalability (Cheemakurthi et al., 2023; IBM, 2025). False positives persist as a known limitation in both Deep Learning (DL) and hybrid AI systems, highlighting the need for balanced approaches (Talaat et al., 2025). Furthermore, recent high-profile regulatory fines against financial institutions underscore the importance of explainability and bias mitigation in AI systems (Emanuel-Burns, 2024; Fitzpatrick, 2024). These trends collectively support the prediction that future fraud detection will increasingly rely on hybrid models that blend Machine Learning (ML), Deep Learning (DL), and rule-based systems for optimal performance and compliance.

Performance Across Different AI Models:

Preliminary expectations suggest:

- Deep Learning (DL) outperforms traditional Machine Learning (ML) models, but Machine Learning (ML) models will be more popular due to their lower computational cost, ease of integration, and interpretability.
- Deep Learning (DL) models handle large datasets efficiently, reducing false positives.
- False positives remain a challenge, especially in advanced AI models.
- The result will indicate a need for hybrid AI models (ML + DL + rule-based detection) and will offer optimal fraud detection by integrating multiple detection methodologies.

Regulatory & Compliance Challenges:

Expected regulatory challenges include:

- Increased scrutiny of AI models for fairness and bias mitigation.
- Major financial institutions face penalties for AI fraud detection failures.
- The necessity for explainability in AI decisions to comply with regulatory requirements.

Enforcement Outcomes and Regulatory Failures:

The comparative analysis that follows will further assess and evaluate the hypothesized impact of the conceptual model introduced earlier, which positions institutional decision-making as a balance between technical model performance, operational feasibility, and compliance risk. The following tables summarize key findings across AI model performance and regulatory outcomes based on the reviewed sources.

Performance Across Different AI Models

This assessment of model limitations further supports the conceptual model's view that detection accuracy alone is insufficient; institutions must also evaluate how each model aligns with interpretability needs and evolving regulatory expectations.

Table 1 AI Model Effectiveness in Fraud Detection

AI Model	Detection Speed	False Positives	Industry Effectiveness Rating
Machine Learning (ML)	Fast	Medium	High
Deep Learning (DL)	Very Fast	Medium	Very High
Natural Language Processing (NLP)	Medium	Low	Medium

Table 2 AI Adoption for Fraud Detection

AI Model	Adoption Rate (%)
Machine Learning (ML)	94%
Deep Learning (DL)	67%
Natural Language Processing (NLP)	72%

The performance thresholds reflected in Table 1 are informed by operational standards in real-time fraud detection environments. Real-time fraud detection systems often require sub-second response times to avoid delays in transaction processing, particularly in mobile and card-present environments. Meanwhile, elevated false positive rates — where legitimate transactions are mistakenly flagged—can lead to costly manual reviews, customer dissatisfaction, and operational delays. These qualitative benchmarks provide a practical lens to assess how AI models perform under real-world financial constraints.

According to Tables 1 and 2, the data highlights that Machine Learning (ML) is the most widely used AI technique in fraud detection, with an adoption rate of 94%. However, the data also emphasize that Deep Learning (DL) models are highly effective, but not yet widely adopted (67%). The Natural Language Processing (NLP) technique received relatively lower ratings from institutions, with the lowest rating across three metrics. While the model indicates strong daily savings, these gains can be rapidly offset by regulatory penalties when AI systems fail to meet

compliance standards. As seen in Table 3, institutions have incurred AML-related fines ranging from $60 million to over $4 billion, often due to weaknesses in oversight, explainability, or data governance.

Regulatory & Compliance Challenges

While the conceptual model highlights the financial value of AI adoption, it also underscores the potential risks when governance mechanisms fail. The following enforcement data illustrates how lapses in explainability, data quality, or oversight can lead to substantial regulatory fines, even when advanced AI systems are in place.

Table 3 Timeline for Regulatory Fines for AI-Related Fraud Detection Failures

Years	Company/Institution	Fine Amount ($)	Regulatory Violation
2022	Global AML Fines (Various Banks)	~$5 Billion	Anti-Money Laundering Violations
2022	Morgan Stanley	$60 Million	Data Security Failures
2023	Deutsche Bank	$186 Million	AML Shortcomings
2023	Binance	$4.3 Billion	AML Violations
2024	City National Bank	$65 Million	AML Violations
2024	Toronto-Dominion Bank (TD Bank)	$3.0 Billion	AML Violations
2025	Paypal	$2.0 Million	Fined by New York's Department of Financial Services for cybersecurity failures that exposed customers' Social Security numbers
2025	OKX (Aux Cayes Fintech Co. Ltd)	$504 Million	AML Violations - failing to prevent criminals from using its services.

Although Table 3 includes examples from international entities, they are presented to illustrate global enforcement trends and underscore the importance of regulatory compliance,

which remains the primary focus of this U.S.-centered analysis. From Table 3, it is noteworthy that regulatory fines for AI fraud detection failures are varied in materiality. Satisfying AML compliance requirements remains a significant challenge for the development of AI-driven fraud detection for financial institutions. It appears that financial institutions were fined the most under this regulation. This finding highlights the importance of integrating effective AI-related fraud detection systems. It also highlights the crucial element of continuous improvement for fraud detection systems to meet the standards of regulatory compliance.

Overall, the ultimate purpose of this section is to assess and evaluate the effectiveness of AI-powered fraud detection systems in financial institutions. The paper seeks to answer the question: To what extent are AI-powered systems improving fraud detection outcomes, and where do gaps remain? The conceptual model presented earlier demonstrates that under optimal conditions, AI systems can generate significant daily cost savings—approximately $71,510 per day, or $17.9 million annually—through fraud loss prevention and reduced operational expenses. However, as this analysis also shows, model-level improvements and cost efficiencies are not sufficient on their own. True effectiveness also hinges on institutional oversight, model interpretability, and regulatory compliance, which continue to present substantial challenges. Institutions that overlook explainability and compliance integration may ultimately face enforcement actions that would offset the operational savings from AI implementations. The high cost of enforcement actions, as outlined in Table 3, highlights the need for financial institutions to treat AI not just as a tool for automation but as a system that must be continuously audited, governed, and aligned with legal standards.

IV. Analysis and Interpretation of Results

Analytical Summary of Findings

The analysis of AI model performance indicates that while Machine Learning (ML) models have the highest adoption rate, they are not always the most effective at detecting complex fraud patterns. Evidently, Machine Learning (ML) models were rated behind Deep Learning (DL) models in both metrics of detection speed and effectiveness rating. While Deep Learning (DL) models demonstrate superior detection speed and accuracy, which makes them more suitable for large-scale fraud detection and prevention, the lower adoption rate suggests that financial institutions may face challenges related to computational costs and regulatory compliance in implementing this model. Natural Language Processing (NLP) models also prove effective in fraud detection, but their scalability limitations hinder broader implementation, resulting in underwhelming results in all metrics compared to Machine Learning (ML) and Deep Learning (DL). Additionally, the challenge of eliminating false positives remains persistent with AI-powered fraud detection systems at financial institutions, as evidenced by the fact that none of the ratings for all AI model performance were above medium. While it is an interesting finding, it aligns with our original expectations due to the need for continuous optimization in these AI models.

Regulatory and compliance challenges emerge as critical findings in the study, particularly with respect to AML compliance. It was a noteworthy finding, as it demonstrates the importance regulators and enforcers place on the effectiveness of these AI-powered fraud detection systems. The increasing number of fines levied against major banks and fintech companies, such as Binance, Deutsche Bank, and TD Bank, underscores the importance of prioritizing regulatory

compliance in AI-driven fraud detection strategies. The high materiality of these fines and penalties indicates how regulators perceive deficiencies and breaches within these detection systems. Many financial institutions have been compelled to reassess AI-based voice verification due to heightened fraud risks, underscoring the need for models that strike a balance between efficiency and compliance with regulatory frameworks (BioCatch, 2024). As a result, financial institutions are implementing multiple security measures to update their detection and prevention systems in conformity with regulatory compliance. Additional security measures include biometrics, multi-factor authentication, device fingerprints, knowledge-based authentication, document verification, and behavioral biometric intelligence (BioCatch, 2024). With the increase in sophisticated and intricate financial crimes, the finding further emphasizes the need to improve these AI models. AI is expected to impact several areas of financial crime prevention strategies, from detection to compliance.

These findings also align closely with the study's conceptual model, which frames AI fraud detection performance as the product of interactions between technical capability, institutional readiness, and regulatory pressure. The model illustrates how AI-driven fraud detection can yield substantial benefits, such as an estimated $71,510 in net daily savings through reduced fraud losses and operational efficiencies. However, it also cautions that these benefits can be quickly negated by compliance failures and regulatory penalties, as evidenced by recent high-profile enforcement actions. For example, even with strong model performance, institutions that fail to implement sufficient oversight, ensure explainability, or manage false positives risk multi-million-dollar fines that far outweigh operational gains. The model further underscores that successful AI deployment must go beyond algorithmic performance; it must be embedded within a governance framework supported by human oversight and internal audit. In this way, the conceptual model provides a useful interpretive lens for understanding how AI systems function not only as technical solutions but as dynamic components of a complex financial, ethical, and regulatory ecosystem.

Implications of the Results

Recent research by Talaat et al. (2025) introduced RiskNet, a modular fraud detection framework that integrates feature selection and explainable AI. Their results demonstrated superior accuracy and interpretability compared to traditional ML models, reinforcing the need for hybrid, transparent systems in financial fraud detection. Similarly, Boudreaux (2025) emphasizes the importance of mutual dependence between humans and AI, arguing that effective oversight and collaboration are essential for managing AI-driven systems in high-stakes environments.

For Financial Institutions & Banks

For financial institutions and banks, the findings highlight the need for strategic investment in AI fraud detection systems. While AI can significantly enhance the accuracy and efficiency of fraud detection, financial institutions must focus on minimizing false positives to prevent customer dissatisfaction and unnecessary transaction blocks. The results of the study suggest that hybrid AI models, incorporating Machine Learning (ML), Deep Learning (DL), and traditional rule-based detection, will provide a more balanced approach to fraud prevention. It is an intricate combination of the most effective aspects of each model. For instance, financial institutions should focus on cultivating the fraud detection effectiveness from Deep Learning (DL) techniques while maintaining the integration of the Machine Learning (ML) model (refer to Table 1). Hybrid models

that combine both Deep Learning (DL) and traditional Machine Learning (ML) approaches need to be explored to determine if they can leverage the strengths of both methodologies to enhance predictive accuracy (Bengani, 2024). Likewise, financial institutions can determine which AI models are best suitable for which type of financial crime. Hybrid learning systems will be a significant leap forward in our quest to make AI more versatile, interpretable, and efficient (Bengani, 2024). Banks should fully leverage AI functionalities to enhance their decision-making processes. It can ultimately lead to a reduction in unnecessary transaction blocks and an improvement in customer experience. It is essential to preserve a balance between technology and human oversight, as fully automated systems may fail to capture nuanced fraudulent behaviors (Steinhaeuser, 2024). Moreover, financial institutions, such as banks, must ensure that AI implementations align with Anti-Money Laundering (AML), General Data Protection Regulation (GDPR), and AI ethics guidelines to avoid legal and financial repercussions. The rise in regulatory fines for non-compliant AI fraud detection systems emphasizes the need for financial institutions to integrate AI solutions that align with evolving legal frameworks such as the GDPR, EU AI Act, and Anti-Money Laundering (AML) laws (refer to Table 2). Institutions that fail to ensure compliance risk substantial financial penalties and reputational damage. The adoption of hybrid AI models that integrate multiple detection methodologies could improve fraud detection efficiency while maintaining regulatory compliance.

For the Detection of Fraudsters & Cybercriminals

For fraudsters and cybercriminals, the increasing sophistication of AI-driven fraud detection presents significant challenges to their illicit activities. However, cybercriminals continue to adapt, leveraging adversarial AI techniques to bypass security measures (Stanham, 2025). While AI-driven real-time fraud detection reduces financial crime rates, adversarial attacks continue to pose a challenge. Cybercriminals can leverage AI-powered tools and Machine Learning (ML) programs to automate and accelerate various phases of a cyberattack (Stanham, 2025). Fraudsters increasingly use identity-based and social engineering attacks, exploiting API (Application Programming Interface) keys, session cookies, and MFA (Multi-Factor Authentication) bypass techniques (CrowdStrike, 2024). Moreover, there will be additional challenges and difficulties associated with synthetic identity fraud. While Deep Learning (DL) models have demonstrated usefulness in detecting identity fraud, criminals can utilize AI-generated fake identities to manipulate systems, such as those employing Deepfakes technologies (Stanham, 2025). The financial sector must continue to explore and implement more robust verification processes, such as biometric authentication and blockchain-enhanced identity validation. Ultimately, fraudsters will continue to exploit weaknesses in AI models, which require continuous system updates and adaptive fraud prevention strategies. These particular challenges necessitate ongoing improvements in fraud detection processes to stay ahead of evolving threats. Financial institutions must prioritize proactive fraud prevention strategies, including real-time monitoring and adaptive AI models, to mitigate emerging risks.

For Regulators & Policymakers

From a regulatory and policymaking perspective, AI-powered fraud detection systems must be designed with transparency and accountability to reduce algorithmic bias. The increase in fines and penalties for AI-related fraud detection failures underscores the pressing need for clear and

comprehensive regulatory guidelines. Regulators and policymakers must establish standardized compliance frameworks for AI fraud detection to ensure fairness and accountability. It is an imperative and urgent matter for a government that lacks comprehensive AI legislation, such as the US (Simpson, 2023). Currently, the regulation of AI governance in the U.S. is managed by several existing agencies, including the U.S. regulatory agencies (Simpson, 2023). These regulatory agencies have come together to create a collective pledge to battle against discrimination and bias in automated systems. That attempt reflects a proactive approach to ensure that AI technologies do not perpetuate existing inequalities (Simpson, 2023). However, financial regulators must establish stricter compliance frameworks to ensure the ethical deployment of AI in fraud detection. Explainability in AI decision-making is particularly critical, as opaque models can lead to unjustified transaction rejections and potential discrimination. Requiring financial institutions to implement explainable AI models would enhance trust in AI-driven security measures while improving regulatory compliance. Transparency is essential for strengthening public trust and guaranteeing fair treatment of customers flagged for fraudulent activities.

In summary, AI-powered fraud detection has made significant strides in enhancing financial security and prevention, but regulatory compliance remains a crucial determinant of its effectiveness. There are still challenges related to false positives, model bias, and compliance that remain as areas for improvement. A hybrid AI model is a viable solution worth considering to achieve higher accuracy and efficiency. Financial institutions must navigate the dual challenge of technological innovation and stringent regulatory oversight to maintain the integrity of their fraud detection systems. Policymakers should work closely with financial institutions to develop the most effective approaches and practices for AI implementation that strike a balance between innovation and compliance. By continuously refining AI models, implementing transparent decision-making frameworks, and aligning with regulatory standards, the financial sector can harness AI's full potential to combat financial fraud efficiently and fairly.

V. Discussion

What can be improved for AI-Powered Fraud Detection Systems?

Data quality

The findings of this study highlight the growing reliance of financial institutions on AI-powered fraud detection systems, underscoring both their effectiveness and the challenges they present. The analysis of various AI models, including Machine Learning (ML), Deep Learning (DL), and traditional rule-based, demonstrates that hybrid approaches tend to offer the most balanced fraud detection outcomes. While AI has significantly improved real-time fraud detection and reduced financial crime incidents, its limitations, such as false positives and adversarial attacks, necessitate further advancements. The accuracy and effectiveness of AI-powered fraud detection systems are heavily dependent on the quality of the data they analyze (Gupta, 2024). Inconsistent, incomplete, or biased datasets can lead to inaccurate fraud detection, resulting in both increased false positives and false negatives. AI-powered fraud detection systems utilize and learn from transaction data, user activity logs, and third-party data sources, including credit reports and geolocation services (Gupta, 2024). Financial institutions must implement robust data validation and cleansing processes to ensure that AI models are trained on high-quality, representative data. It is critical to ensure that inadequate data are eliminated, as they have an adverse influence on fraud algorithm

predictions and signal detection (Gupta, 2024). Additionally, a collaboration between financial institutions and regulators can help establish standardized data-sharing practices that enhance the accuracy of fraud detection while maintaining privacy and compliance.

Roles of Internal Audits in AI Fraud Detection

Regulatory compliance remains a critical issue as financial institutions face increasing scrutiny regarding AI bias, transparency, and explainability. The increase in regulatory fines for AI compliance failures underscores the need for a more structured and standardized regulatory framework. It is not only designed for the effectiveness of AI fraud detection models but also ensures ethical soundness and compliance with legal requirements. Since there is a lack of comprehensive AI legislation in the US, the role of internal auditors in AI fraud detection is also crucial in confirming that the AI models are reasonably assured (Simpson, 2023). Internal auditors provide an additional layer of oversight by testing whether AI fraud detection systems are functioning as intended, free from significant biases, and aligned with regulatory requirements (TeamMate, 2025). They play a crucial role in evaluating AI-driven fraud models, identifying shortcomings, and providing recommendations for refinements. Financial institutions must strengthen their internal audit mechanisms to regularly evaluate AI fraud detection systems, ensuring transparency, compliance, and reliability, in line with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (TeamMate, 2025).

For example, the Office of the Comptroller of the Currency (OCC) requires national banks to maintain effective internal audit functions that assess the adequacy of risk management systems, including those involving AI. Similarly, the Federal Reserve's supervisory guidance emphasizes the role of internal audit in evaluating model risk management frameworks, particularly for AI-driven systems used in fraud detection. These agencies expect internal auditors to independently validate AI models, assess compliance with regulatory expectations, and ensure that governance structures are in place to manage AI-related risks.

Additionally, internal auditors are responsible for ensuring compliance with data security and regulatory requirements, including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Payment Card Industry Data Security Standard (PCI DSS) (TeamMate, 2025). As AI models are increasingly subject to regulatory scrutiny, auditors must ensure that these systems operate transparently and fairly, thereby mitigating risks associated with algorithmic bias and discriminatory decision-making. To improve AI fraud detection, auditors also contribute to continuous model improvements. By examining audit findings, financial institutions can refine their AI algorithms, optimize fraud detection parameters, and implement corrective measures to address vulnerabilities in their systems. Internal auditors can further ensure the data quality used in building these AI models. Internal auditors can ensure datasets are complete, up-to-date, and free from biases that could impact fraud detection outcomes (TeamMate, 2025). Overall, internal auditors serve as a bridge between AI developers, compliance teams, and senior management, facilitating a well-integrated approach to AI governance. Their role in conducting independent evaluations and fostering accountability ensures that AI fraud detection remains both effective and ethical.

What are other challenges in AI that have implications for fraud detection?

AI fraud detection models, particularly Machine Learning (ML), Deep Learning (DL), and traditional rule-based, demonstrate varying levels of effectiveness. Hybrid AI approaches could show promise in enhancing fraud detection accuracy (Bengani, 2024). However, model limitations such as overfitting, lack of interpretability, and high computational costs present challenges for widespread adoption. Future research should focus on optimizing AI algorithms to minimize false positives and enhance real-time detection capabilities while reducing operational burdens on financial institutions. One of the challenges in AI-powered fraud detection is model interpretability. Many advanced AI models, such as Deep Learning (DL) and Neural Networks, operate as 'black boxes,' making it difficult for financial institutions to understand how decisions are made (Ducret, 2025). This lack of transparency can create trust issues for both regulators and customers, especially in cases where transactions are flagged as fraudulent without clear explanations. Enhancing model interpretability through Explainable AI (XAI) techniques is crucial to gaining regulatory and public trust while ensuring compliance with governance requirements (IBM, 2025). Financial institutions can also allow internal auditors to support and approve the use of explainable AI techniques, which provide a straightforward understanding of how fraud detection decisions are made (TeamMate, 2025).

Moreover, AI fraud detection systems must navigate complex ethical concerns, particularly those related to bias and fairness. If trained on biased datasets, AI models may disproportionately target certain demographic groups, leading to financial exclusion or unjust scrutiny (Ducret, 2025). When detection systems examine financial transactions or assess high-risk customers, the possibility of biased decisions, whether from data on demographics, socioeconomic elements, or historical data patterns, can be profound and unintentional (Ducret, 2025). This ethical concern is particularly relevant for financial institutions, as AI-driven determinations can impact decisions and conclusions that have financial implications for their consumers. To manage these challenges, financial institutions must ensure that AI models are trained on diverse, representative datasets and continually scrutinize their outputs for indications of bias (Ducret, 2025). If these systems are not ready in the short term, human oversight can play a critical role in the decision-making process. Additionally, ethical concerns arise regarding data privacy, as AI fraud detection relies on a vast collection of transactional and behavioral data (Ducret, 2025). Financial institutions must implement rigorous ethical frameworks to prevent bias and ensure AI decisions are aligned with transparency and privacy requirements (Ducret, 2025).

Limitations of this Research

While this study offers valuable insights into AI-powered fraud detection, several limitations should be acknowledged. One key limitation is the availability of comprehensive data from financial institutions. Many financial institutions do not publicly disclose or publish detailed fraud detection information due to concerns about confidentiality and competitive considerations. As a result, this research relies on publicly available industry reports and case studies, which may not fully capture the nuances of fraud detection effectiveness across different financial sectors. For instance, there is a lack of some AI fraud detection metrics, such as accuracy rates across different financial institutions and Graph Neural Networks' adoption. Likewise, another limitation pertains to the generalization of AI model performance. The effectiveness of AI-driven fraud detection varies based on the type of financial fraud being studied, such as credit card fraud, money

laundering, or transaction fraud. While this study extensively discusses AI performance, it does not delve deeply into specific fraud categories, which may limit the applicability of its findings to highly specialized financial crimes.

Additionally, this study highlights challenges in measuring AI bias and fairness (Adhikari et al., 2024). AI fraud detection models are susceptible to biases inherent in the datasets they are trained on, which can result in excessive targeting of specific demographics. However, quantifying and mitigating AI bias remains complex due to the lack of widely available demographic data in fraud detection systems. Further research is needed to comprehensively assess AI fairness. Moreover, regulatory uncertainty poses a significant challenge to the implementation of AI fraud detection. AI-related regulations are continuously evolving, with different jurisdictions adopting varied compliance standards. While this study examines available and relevant regulatory frameworks, future legislative changes could significantly impact how AI fraud detection systems operate and comply with laws such as GDPR, AML regulations, and AI ethics guidelines (Simpson, 2023).

Opportunities for further research

Despite the significant advancements in AI fraud detection, several areas warrant further exploration to enhance the effectiveness, fairness, and adaptability of these systems. One promising area for future research is the development of defense mechanisms against adversarial AI. As fraudsters increasingly leverage AI-driven attacks, financial institutions must explore methods to counter adversarial AI threats. Research into robust machine learning models that can detect and adapt to adversarial manipulation will be crucial in maintaining the efficiency of fraud detection. Since Graph Neural Networks (GNNs) data is lacking, it suggests a gap in industry-wide adoption or available research. The lack of GNN-related data presents an opportunity for further research into its effectiveness in fraud detection. It would provide additional insights into the effectiveness of AI models with Graph Neural Networks (GNNs) compared to other approaches, such as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP). Additionally, improving AI explainability and interpretability remains a crucial research priority. Explainable AI (XAI) can help financial institutions better understand AI-driven fraud detection decisions, reducing bias and increasing regulatory compliance (IBM, 2025). Future studies should investigate techniques to enhance AI transparency, thereby making fraud detection models more comprehensible to regulators and financial institutions alike. Another critical area is the study of AI bias mitigation strategies. Ensuring that AI fraud detection models do not disproportionately impact certain demographics is crucial for ethical AI adoption. Research should focus on developing unbiased training datasets, fairness-aware algorithms, and standardized frameworks for auditing bias to address these concerns effectively.

While blockchain technology has been around for over a decade, its applications continue to expand and evolve. There is still ongoing research on optimizing its security, scalability, and integration with other technologies (such as AI) is ongoing. The integration of AI and blockchain in fraud detection systems is important due to the complementary strengths of both technologies. It further presents a promising area for further research. Recent studies, such as those by Ketha and Provodnikova (2024), highlight the need for further research and investigation into AI-blockchain integration as a comprehensive strategy for fraud detection in financial transactions. The paper highlights how blockchain's decentralized and tamper-resistant ledger can ensure secure and transparent data. The authors explain how AI excels at identifying patterns and anomalies

indicative of fraud. The authors propose a framework that can leverage both technologies to improve fraud detection and reduce vulnerabilities (Ketha and Provodnikova, 2024).

By exploring these research opportunities, financial institutions, regulators, and AI researchers can collaborate to develop more robust, ethical, and efficient fraud detection systems that keep pace with the evolving landscape of financial crime.

VI. Conclusion

AI-powered fraud detection has revolutionized financial crime prevention by improving precision, efficiency, and real-time monitoring abilities. However, its across-the-board implementation is followed by challenges that financial institutions must address to maximize its benefits while mitigating risks. As the primary goal of this paper is to suggest the next step for AI-powered fraud detection systems, the research findings indicate that hybrid AI models, which integrate Machine Learning (ML), Deep Learning (DL), and traditional rule-based techniques, offer the most comprehensive approach to fraud detection. Financial institutions must continually adapt their AI models to combat evolving fraud tactics and approaches. Investing in Explainable AI (XAI) to improve transparency and regulatory compliance will provide more meaningful insights to all stakeholders. Collaboration with regulatory bodies is necessary to ensure that AI-driven fraud detection meets both ethical and legal standards while maintaining public trust. Looking ahead, further research should explore the role of adversarial machine learning in fraud prevention, as well as the use of Graph Neural Networks (GNNs), to ensure that AI systems remain effective against AI-powered fraud attacks.

In conclusion, while AI-powered fraud detection systems provide a strong foundation for mitigating financial crime, they are not foolproof. Ongoing advancements, regulatory frameworks, and ethical considerations will play a crucial role in shaping the future effectiveness of these systems. The integration of explainable, adaptive, and ethically governed AI solutions will be key to ensuring the long-term success of AI-powered fraud prevention in financial institutions. A proactive and collaborative approach between financial institutions, regulators, internal auditors, and AI researchers will be necessary to create a secure and effective fraud detection ecosystem. Ultimately, this paper contributes to the academic discourse by linking AI model performance to regulatory compliance and institutional implementation challenges. Its practical insights offer guidance for financial institutions navigating the evolving fraud landscape and for policymakers seeking to develop adaptable, enforcement-ready governance frameworks. As such, the findings serve as both a roadmap for institutional innovation and a call to action for future research in AI fraud governance.

References

ABA Banking Journal. (2024, March 4). City National Bank agrees to pay $65 million to resolve risk control allegations. https://bankingjournal.aba.com/2024/03/city-national-bank-agrees-to-pay-65-million-to-resolve-risk-control-allegations/

Adhikari, P., Hamal, P., & Baidoo Jnr, F. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive, 13 (1)*, 1457–1472. https://doi.org/10.30574/ijsra.2024.13.1.1860

Bengani, V. (2024). Hybrid Learning Systems: Integrating Traditional Machine Learning with Deep Learning Techniques. ResearchGate. https://doi.org/10.13140/RG.2.2.10461.22244/1

BioCatch. (2024). 2024 AI Fraud Financial Crime Survey. https://www.biocatch.com/ai-fraud-financial-crime-survey

Boudreaux, M. (2025). Mutual dependence and vulnerability in human and AI futures. RAND Corporation. https://www.rand.org/pubs/working_papers/WRA1234-1.html

Butler, R. B. (2024, September 30). How AI can help law enforcement fight fraud & other crimes. Thomson Reuters. https://www.thomsonreuters.com/en-us/posts/government/ai-law-enforcement-fraud/

Cheemakurthi, S. K. M., Kilaru, N. B., & Gunnam, V. (2023). Ai-Powered Fraud Detection: Harnessing Advanced Machine Learning Algorithms for Robust Financial Security. *International Journal of Advances in Engineering and Management, 5(4)*, 1907–1915. https://ijaem.net/issue_dcp/Ai Powered Fraud Detection Harnessing Advanced Machine Learning Algorithms for Robust Financial Security.pdf

Core Payment Solutions. (2024, June 28). What fraud prevention features should a POS system have? https://corepaymentsolutions.com/what-fraud-prevention-features-should-a-pos-system-have/

Cornerstone. (2025, June 5). The crucial role of humans in AI oversight. https://www.cornerstoneondemand.com/resources/article/the-crucial-role-of-humans-in-ai -oversight/

Crane, V., & Kimbrell, T. (2025). Anti-money laundering (AML). FINRA. https://www.finra.org/rules-guidance/key-topics/aml

CrowdStrike. (2024). CrowdStrike 2024 Global Threat Report. https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

Dhrangadhariya. (2025, March 1). The role of Artificial Intelligence (AI) in internal auditing: Transforming risk and compliance. CSM & CO LLP. https://www.csmllp.in/the-role-of-artificial-intelligence-ai-in-internal-auditing-transforming-risk-and-compliance/

Ducret, J. (2025, January 27). AI in fraud detection and due diligence: Top 8 ethical implications. TenIntelligence. https://tenintel.com/ai-fraud-detection-due-diligence/

Emanuel-Burns, C. (2024, October 14). TD Bank hit with $3bn in fines over AML failures - fintech futures: Fintech News. FinTech Futures. https://www.fintechfutures.com/regulatory-actions/td-bank-hit-with-3bn-in-fines-over-aml-failures

Federal Deposit Insurance Corporation. (2004). Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control. Federal Deposit Insurance Corporation (FDIC). https://www.fdic.gov/resources/supervision-and-examinations/examination-policies-manual/section8-1.pdf

Financial Crimes Enforcement Network. (2025). Financial institution definition. FinCEN.gov. https://www.fincen.gov/financial-institution-definition

Fitzpatrick, C. (2024, October 4). The impact of AI on Fraud Detection Systems. Planet Compliance. https://www.planetcompliance.com/ai-compliance/ai-fraud-detection-systems/

Flinders, M., Smalley, I., & Schneider, J. (2025, April 30). AI fraud detection in banking. IBM. https://www.ibm.com/think/topics/ai-fraud-detection-in-banking

Georgiev, M. (2024, August 1). Shielding retailers from credit card fraud: A comprehensive guide. NRS Pay. https://nrspay.com/2023/10/02/shielding-retailers-from-credit-card-fraud-a-comprehensive-guide/

Gupta, P. (2024, November 11). Data Engineering challenges in handling large volumes of fraud detection data. MRC. https://merchantriskcouncil.org/learning/resource-center/member-news/blog/2024/discover-data-engineering-challenges-in-handling-large-volumes-of-fraud-detection-data

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of ai-enhanced techniques in credit card fraud detection. *Journal of Big Data, 12(1)*. https://doi.org/10.1186/s40537-024-01048-8

Hayes, A., Kelly, R., & Kvilhaug, S. (2024, February 25). What is a financial institution?. Investopedia. https://www.investopedia.com/terms/f/financialinstitution.asp

Hickman, T. H., Lorenz, S., Teetzmann, C., & Jha, A. (2024, July 16). Long awaited EU AI Act becomes law after publication in the EU's Official Journal. White & Case LLP. https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal

Hodge, N. (2024, June 10). The fraudsters have AI, too. Theiia - Internal Auditor. https://internalauditor.theiia.org/en/articles/2024/june/the-fraudsters-have-ai-too/

IBM. (2025, February 13). What is explainable AI (XAI)? https://www.ibm.com/think/topics/explainable-ai

Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine Learning. *Journal of Economics, Finance and Accounting Studies, 6(1)*, 67-77. https://doi.org/10.32996/jefas.2024.6.1.7

Ketha, S., & Provodnikova, A. (2024, December 2). Combining Blockchain and AI for Fraud Detection: Building Secure, Transparent, and Sustainable Financial Ecosystems. *Global Journal of Business and Integral Security.* https://gbis.ch/index.php/gbis/article/view/599/500

Kurnia, P., & Yuniarti, R. (2024). Analysis of Fraud Diamond Theory in Detecting Fraudulent Financial Statement: Study in Manufacturing Company in Indonesia. *Dinasti International Journal of Economics, Finance & Accounting, 5(5)*, 5468–5478. https://doi.org/10.38035/dijefa.v5i5.3572

Levitt, K. (2024, December 5). How is AI used in fraud detection? NVIDIA Blog. https://blogs.nvidia.com/blog/ai-fraud-detection-rapids-triton-tensorrt-nemo/

Louati, H., Louati, A., Almekhlafi, A., ElSaka, M., Alharbi, M., Kariri, E., & Altherwy, Y. N. (2024). Adopting Artificial Intelligence to Strengthen Legal Safeguards in Blockchain Smart Contracts: A Strategy to Mitigate Fraud and Enhance Digital Transaction Security. *Journal of Theoretical & Applied Electronic Commerce Research, 19(3),* 2139–2156. https://doi-org.libproxy.scu.edu/10.3390/jtaer19030104

Lumenova AI. (2024, September 17). The strategic necessity of human oversight in AI Systems. https://www.lumenova.ai/blog/strategic-necessity-human-oversight-ai-systems/

Mastercard. (2024, January 24). Industry perspectives on AI and transaction fraud detection: Brighterion AI: A MasterCard Company. Brighterion AI | A Mastercard Company. https://b2b.mastercard.com/news-and-insights/blog/industry-perspectives-on-ai-and-transaction-fraud-detection/

Mayfield, J. M. (2024, August 20). As nationwide fraud losses top $10 billion in 2023, FTC steps up efforts to protect the public. Federal Trade Commission.

https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

Olowu, O., Adeleye, A. O., Omokanye, A. O., Ajayi, A. M., Adepoju, A. O., Omole, O. M., & Chianumba, E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *GSC Advanced Research and Reviews, 21(2),* 227–237. https://doi.org/10.30574/gscarr.2024.21.2.0418

Pavion. (2024, April 26). The role of AI in fraud detection for retail businesses. Pavion. https://pavion.com/resource/the-role-of-ai-in-fraud-detection-for-retail-businesses/

Petraşcu, D., & Tieanu, A. (2014). The role of Internal Audit in Fraud Prevention and Detection. *Procedia Economics and Finance, 16*, 489–497. https://doi.org/10.1016/s2212-5671(14)00829-6

Reeder, S. (2025). 10 common financial scams: UW Credit Union: UW Credit Union. UW Credit Union. https://www.uwcu.org/online-banking/articles/10-scams/

Rodgers, W., Murray, J. M., Stefanidis, A., Degbey, W. Y., & Tarba, S. Y. (2023). An artificial intelligence algorithmic approach to ethical decision-making in Human Resource Management Processes. *Human Resource Management Review, 33(1)*, 100925. https://doi.org/10.1016/j.hrmr.2022.100925

Simpson, W. (2023, August 2). AI regulatory enforcement around the world. International Association of Privacy Professionals (IAPP). https://iapp.org/news/a/ai-regulatory-enforcement-around-the-world

Stanham, L. (2025, January 16). Most common AI-powered cyberattacks . CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

Steinhaeuser, I. (2024, December 23). How AI will disrupt fraud prevention & detection technologies . Thomson Reuters Institute. https://www.thomsonreuters.com/en-us/posts/corporates/technological-considerations-fraud-prevention/

Stempel, J. (2022, January 3). Morgan Stanley to pay $60 mln to resolve data security lawsuit | Reuters . Reuters. https://www.reuters.com/markets/funds/morgan-stanley-pay-60-mln-resolve-data-security-lawsuit-2022-01-02/

Stempel, J. (2025, January 23). PayPal fined by New York for cybersecurity failures. Reuters. https://www.reuters.com/technology/paypal-fined-by-new-york-cybersecurity-failures-2025-01-23/

Talaat, F. M., Medhat, T., & Shaban, W. M. (2025). Precise fraud detection and risk management with explainable artificial intelligence. Neural Computing and Applications. https://link.springer.com/article/10.1007/s00521-025-11396-y

TeamMate. (2025, February 19). Internal Audit's role in AI Fraud Detection. Wolters Kluwer. https://www.wolterskluwer.com/en/expert-insights/internal-audits-role-ai-fraud-detection

U.S. Department of Justice. (2025, January 31). Financial fraud crime victims. United States Attorney's Office Western District of Washington. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud

United States Department of Justice. (2025, February 24). Okx pleads guilty to violating U.S. anti-money laundering laws and agrees to pay penalties totaling more than $500 million. United States Department of Justice, Southern District of New York. https://www.justice.gov/usao-sdny/pr/okx-pleads-guilty-violating-us-anti-money-laundering-laws-and-agrees-pay-penalties

Valleskey, B. (2024, July 11). The rise of AI fraud Agents. Inscribe. https://www.inscribe.ai/ai-for-financial-services/ai-fraud-agents/

West, A., & Ciais, F. (2023, December). Impact of artificial intelligence on fraud and scams. PwC. https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf

Yuhertiana, I., & Hadi Amin, A. (2024). Artificial Intelligence Driven Approaches for Financial Fraud Detection: A systematic literature review. KnE Social Sciences. https://doi.org/10.18502/kss.v9i20.16551