

## From Manual to Automated Fraud Reporting in U.S. Financial Institutions: Change Management Strategies and Measurable Impact - A Narrative Review

Cecilia Wanjiku Kamau<sup>1</sup>, Matthew Oman-Amoako<sup>2</sup>

<sup>1</sup>Independent Researcher

<sup>2</sup>Department of Business Administration – Accra Institute of Technology, Ghana

**KEYWORDS:** Fraud Reporting Automation, Suspicious Activity Reports, Financial Institutions, Change Management.

**Corresponding Author:**  
Cecilia Wanjiku Kamau

**Publication Date:** 19 September-2026  
**DOI:** [10.55677/GJEFR/03-2026-Vol03E9](https://doi.org/10.55677/GJEFR/03-2026-Vol03E9)

**License:**  
This is an open access article under the CC BY 4.0 license:  
<https://creativecommons.org/licenses/by/4.0/>

### ABSTRACT

For many years, U.S. financial institutions have relied on manual, investigator-based workflows to generate Suspicious Activity Reports (SARs). In today's era of financial crime, filing of SARs under the Bank Secrecy Act (BSA) continues to be inefficient, time-consuming, and prone to error. Manual reporting is a huge challenge as consumers report \$12.5 billion in fraud losses in 2024 and financial institutions report more than 4 million SARs each year. Today, institutions have spent a lot of money on automated fraud detection and RegTech solutions and yet, despite these investments, not many institutions can reap significant benefits since automated solutions are often thought of as technology solutions, and not as a transformation of the organization, its processes and people. This narrative review collates peer-reviewed literature across the four themes of the organizational and structural drivers for the transition, change management frameworks for adoption, design and governance characteristics of automated systems, and measured business and compliance impact on the transition to automated systems from 2020 until 2026. However, results from the review demonstrate that the ability to implement structured change management, explain systems to the regulator, align the system with the regulation, and measure performance are significant to achieving automation success, and not just the technical capability itself. These results give compliance officers and financial institution executives a single source of evidence to inform their fraud reporting automation investments and maximize impact.

*Cite the Article:* Kamau, C.W., Amoako, M.O. (2026). From Manual to Automated Fraud Reporting in U.S. Financial Institutions: Change Management Strategies and Measurable Impact - A Narrative Review. *Global Journal of Economic and Finance Research*, 3(9), 586-591.  
<https://doi.org/10.55677/GJEFR/03-2026-Vol03E9>

### 1.0 INTRODUCTION

The role of the fraud reporter in the financial institution industry is a pivotal one that is at the nexus of regulatory compliance, financial crime prevention, and the financial institution's operations. The Bank Secrecy Act (BSA) and implementing regulations mandate that covered institutions submit Suspicious Activity Reports (SARs) to the Financial Crimes Enforcement Network (FinCEN) within 30 calendar days of the discovery of potentially reportable activity, and for a period of 30 days after a suspect is

identified, for a total of 60 calendar days (Reports by Banks of Suspicious Transactions, 2024). The number of SARs filed by financial institutions is high, in excess of four million per year, and the U.S. fraud landscape that creates this reporting burden is vast and growing in size and complexity (Fulford, 2026). The Federal Trade Commission (FTC) reported that U.S. consumers incurred a total of \$12.5 billion in direct losses to fraud in 2024, and among the most common types of fraud, wire transfer fraud, account takeover fraud, and scams run by AI are the fastest-growing (Fulford, 2026; Irfan et al., 2025).

Manual fraud reporting is typically how compliance analysts operate, where they review alerts from various transactions, gather documentation, and manually report and draft their SAR narratives. These processes are not optimally designed for the fraud landscape today. Investigators deriving information from tabular alert output are expected to be able to interpret complex and high-volume transaction patterns, make a range of decisions with discretionary judgment on alert thresholds, and create legally compliant narrative documentation in limited time without the benefit of automation (Oyekunle et al., 2025). Consequently, this results in variable SAR quality, higher false negative rates, missed filing deadlines, and skilled compliance staff spending time on mechanical documentation with minimal investigative value.

The challenge encompasses extensive automation requirements. Traditional fraud monitoring systems in U.S. financial institutions detect only 65-70% of fraud and have a high false positive rate, leading to losses for investigators (Sarna et al., 2025). As fraudsters adopt digital currencies, machine learning (ML) techniques have demonstrated surpassing rule-based systems in detecting anomalous crypto transactions (Pocher et al., 2023; Brenner, 2024).

Also, major U.S. banks are transitioning to automated fraud reporting systems utilizing AI, NLP (Natural Language Processing), ML, and RegTech (Regulatory Technology) compliance, as reported by Rafiq & Sohail (2025) and Bagherifam et al. (2025). RegTech adoption also increases the effectiveness of compliance and risk evaluation and decreases operating expenses in banks of the United States (Jeyasingh, 2023). Additionally, the growth of decentralized finance (DeFi) is complicating regulatory frameworks and increasing demand for RegTech as a viable compliance solution, according to Devanga (2023).

Nonetheless, the actual benefits of reporting automation for many institutions remain uncertain. Existing literature addresses this issue in fragments, with some focusing on technical detection algorithm optimization but ignoring organizational adoption (Sarna et al., 2025), while others view digital transformation generically without contextual compliance considerations (Karakuş & Yalçın, 2024; Cosa & Torelli, 2024), and further investigations of RegTech governance lack quantifiable business impact evidence (Bagherifam et al., 2025; Rafiq & Sohail, 2025). No comprehensive synthesis integrates organizational drivers, change management, system design, governance, and financial impact to assess the success of fraud reporting automation in U.S. financial institutions. The tangible impact is evident; institutions invest heavily in automation platforms but fail to achieve anticipated benefits due to inadequate organizational and change management preparation (Tucker, 2024; Rafiq & Sohail, 2025). Therefore, this review aims to address these issues.

## 2.0 LITERATURE SEARCH STRATEGY

This narrative review used the principles of integrative narrative synthesis and was carried out using several academic, regulatory, and specific institutional repositories, such as FinCEN (Financial Crimes Enforcement Network), the FFIEC (Federal Financial Institutions Examination Council), and the FATF (Financial Action Task Force) and PubMed, Google Scholar, Scopus, and SSRN. Articles, theses and dissertations, regulatory publications, and institutional reports published in 2020-2026 were considered for inclusion. The search terms used were various combinations of the following: fraud reporting automation, Suspicious Activity Report (SAR), Suspicious Activity Reports, AML (Anti-Money Laundering) compliance automation, RegTech, SupTech, financial institution digital transformation, change management, machine learning fraud detection, behavioral biometrics, data governance, regulatory technology adoption, financial crime prevention, and U.S. banking compliance. Sources were identified based on relevance to the U.S. financial institution environment and to the problem of automated fraud reporting transitions. Research purported to apply exclusively to international markets or research that only targeted fraud typologies, not institutional reporting processes, were omitted. Sources meeting inclusion criteria were organized thematically across the four domains of the review and are synthesized in the sections below.

## 3.0 DATA SYNTHESIS

This section synthesizes evidence from peer-reviewed literature, regulatory publications, and institutional reports published between 2020 and 2026, organized across four thematic domains that collectively determine the success of fraud reporting automation transitions in U.S. financial institutions: the organizational and structural drivers of the transition, change management frameworks for adoption, design and governance principles for automated systems, and measurable business and compliance impact. Each theme was identified through iterative review of the included literature, with sources assigned to themes based on their primary empirical or theoretical contribution. Together, the four themes form the evidence base for the integrated conceptual framework presented below.

### 3.1 Thematic Findings

#### 3.1.1 Theme 1: Organizational and Structural Drivers of the Transition.

The case for automated fraud reporting in U.S. financial institutions is driven by the need to move from manual to automated SAR processing in tandem with several concurrent pressures, including regulatory, operational and competitive. However, at the regulatory level, the ongoing SAR modernization program by FinCEN is imposing growing requirements on the quality, timeliness and risk-based prioritization of SARs that manual processes are unable to reliably satisfy (Financial Crimes Enforcement Network et al., 2025; Rafiq & Sohail, 2025). The ability to monitor, adapt, and respond to risk data in real time, beyond what is possible through manual means, is essential to risk-based customer due diligence, which forms the basis of successful fraud and financial crime management efforts, and automated systems can no longer be considered a luxury, but rather a requirement, for compliant and risk-calibrated financial crime and fraud reporting (Tucker, 2024).

The problems with manual fraud reports are well reported on operationally. Advanced analytics for fraud detection and financial crime prevention produce measurably better results, such as increased detection rates, quicker turnaround time on alerts and better-quality reports compared to manual methods, stemming from the disconnect between the amount and complexity of today's transaction data and the limited cognitive resources of manual review. Institutions with high false-positive rates also have costs associated with compliance team man-hours, while compliance teams are tasked with combating fraud and must work with a high level of precision. Operational implications for institutions include that behavioral biometrics substantially increase the detection precision while reducing the false-positive rate, which significantly lowers the cost of compliance team man-hours for institutions that have high false-positive rates (Oyekunle et al., 2025). Sarna et al. (2025) provide an overview of fraud detection models based on AI in financial networks and find that the benefits of automation are clear, but the hard part is implementing and adopting it within the organizational context.

The financial and competitive aspect of the organizational driver is also provocative in that banks in the U.S. will be at risk for more than \$200 billion in expected online banking fraud losses from 2020 to 2024, and another \$200 billion in fines for non-compliance since 2008, according to Jeyasingh (2023), which makes a compelling business case for investing in automation. Devanga (2023) pinpoints an increasing trend of DeFi and financial crimes facilitated by cryptocurrency transactions as a structural challenge that manual monitoring efforts cannot overcome at the scale required, while Pocher et al. (2023) showed that machine learning-based forensics can achieve detection performance on cryptocurrency anomalies that cannot be matched by rule-based and manual systems. For instance, Boateng et al. (2025) validate the labor cost argument for automation in the broader context of fraud reporting that carries over to the context of terrorism financing pattern identification in U.S. financial institutions, as they demonstrate that ML models can outperform manual efforts to detect patterns at a much higher rate.

This activity covers aspects of change management frameworks and the successful implementation of change (Karakuş & Yalçın, 2024; Cosa & Torelli, 2024).

#### 3.1.2 Theme 2: Change Management Frameworks for Successful Adoption

The common theme in the literature on fraud reporting automation is that organizational and human-side aspects, rather than technical issues, are the most important factors for determining the success of an automated system in reaching compliance and financial goals (Oyekunle et al., 2025). Organizational barriers are the greatest predictors of RegTech adoption failures in banking, on par with technical and cost constraints, with staff resistance, lack of change leadership, lack of training, and lack of structured adoption strategies standing out as the big ones between failed versus successful implementations (Rafiq & Sohail, 2025). A review of theoretical models and case studies of organizational change management and digital transformation found two of the most frequently referenced models to be Kotter's 8-Step Change Model and the ADKAR model (Awareness, Desire, Knowledge, Ability, Reinforcement) for managing technology adoption in regulated institutional settings (Karakuş & Yalçın, 2024).

Kotter's model is especially applicable for the specific case of fraud reporting automation, with the first stage of the process, a clear and credible sense of urgency, fitting right in with the compliance push that propels the transition. The risks of not reporting fraud and keeping the incidents documented give the urgency case to which Kotter's model needs to move to senior leadership commitment and overcome institutional inertia (Karakuş & Yalçın, 2024). In addition, it is essential to establish a guiding coalition across compliance, technology, operations, and the C-suite to ensure cross-functional alignment and success in the financial institution landscape, where fraud reporting automation touches multiple areas and demands cross-functional alignment and cooperation (Cosa & Torelli, 2024). The systematic review by Cosa and Torelli (2024) found that the lack of cross-functional governance structures is one of the most predictive organizational characteristics of failing digital transformation.

Compliance is a specific area where communication and resistance management need to be looked at in more detail, as investigators and analysts who have developed manual skills in drafting SARs could see automation as a threat to their role value. In this context, resistance management is not achieved by replacing the investigator but by augmenting their role, with automated SAR tools guiding them to focus on case judgment, pattern analysis, and quality control checking instead of tedious data assembly documentation (Irfan et al., 2025). The extent to which organizations systematically build and disseminate digital skills across teams, known as knowledge strategy maturity, is shown to be a key determinant of digital technology performance in the transitions to fraud reporting automation (Ferreira et al., 2024). Role-specific training focused on new skills needed to operate automated SAR processes, like

interpreting risk scores generated by AI, validating narratives generated by NLP, and understanding outputs from explainability, is linked to faster time to competency and fewer system workarounds (Sarna et al., 2025; Oyekunle et al., 2025).

### 3.1.3 Theme 3: Design and Governance Principles for Automated Fraud Reporting Systems

The design and management of automated fraud reporting systems are what will influence the compliance, reliability, and trust of the output by the system within the organization. Explainability, regulatory alignment, and data governance are key concepts that repeatedly appear in the literature as key principles (Pavlidis, 2023; Bagherifam et al., 2025; Oyekunle et al., 2025). In the context of the SAR, explainability is not just a design requirement but also a legal compliance obligation: FinCEN expects that the SAR narrative should include enough factual detail to aid law enforcement investigations, but AI-generated SARs without evidence trails are not considered compliant because they lack explainability even if they are accurate in detecting the suspicious activity. Pavlidis (2023) states that to ensure that AI is used effectively for AML and SAR reporting, organizations must be able to explain the rationale behind the model output to investigators, allowing them to review and confirm findings, and include documentation of the evidence chain in regulatory submissions. The concept of explainability and interpretability is also recognized as a prerequisite for institutional trust in the outputs of AI in the context of online radicalization detection and prevention, an area where the same key machine learning architecture is used for financial crime detection (Berjawi et al., 2023).

The second foundational governance principle is regulatory alignment: the continuous process of aligning automated systems to the latest FinCEN guidance, SAR typology guidance, and examination standards. In their systematic review on RegTech and SupTech governance, Bagherifam et al. (2025) discover that institutions with formal regulatory monitoring protocols such as a designated compliance technology governance committee, regular system audits to check against regulatory requirements, and processes in place to integrate regulatory change into systems, significantly outperform those that consider system configuration a one-off activity. The potential for regulatory drift, caused by the progressive divergence of the automated system's behavior and the changing regulatory requirements, is especially high in the context of fraud reporting, where the SAR filing requirements, typology guidance, and the expectations of examiners are updated regularly (Rafiq & Sohail, 2025; Bagherifam et al., 2025).

The third principle is data governance and it is the most often underestimated one in fraud reporting automation deployments. Oyekunle et al. (2025) prove that to achieve the accuracy that fraud detection automated systems promise, a data governance-based approach is an essential element, including using consistent data taxonomies, behavioral data integrity controls, and role-based access management. Automated systems are only as reliable as the underlying information and the data used to analyze transactions and customers; inconsistent data definitions, missing relationship data, and integration gaps with delays in data help to hinder the accuracy of detection and the completeness of SARs. In the customer due diligence (CDD) context, studies posit that investments in data infrastructure are essential for a risk-based approach to fraud and financial crime management that needs to be made before or in parallel with the deployment of automation (Tucker, 2024; Oyekunle et al., 2025). Also, Brenner (2024) further discusses interoperability issues on the blockchain and DeFi space as data governance problems that introduce systematic blind spots in automated fraud monitoring.

### 3.1.4 Theme 4: Measurable Business and Compliance Impact

The business and compliance impact of automated fraud reporting systems, when implemented within well-governed, change-managed transitions, is substantial and consistently documented across multiple dimensions: detection accuracy, SAR filing timeliness, compliance cost reduction, false positive rates, and investigative productivity. The consistent finding is that detection accuracy is improved, reporting that modern AI-based fraud detection models in financial networks have significantly higher detection rates and lower false-positive rates than their rule-based counterparts, with detection rates ranging from 87% to 94% for AI models versus 65% to 70% for manual models, and false positive reductions of 40–60% (Sarna et al., 2025). If false positive investigation is a large percentage of your compliance team's effort, a 40% to 60% reduction in false positives directly affects your investigative capacity and allows your team to focus on more important tasks (Oyekunle et al., 2025).

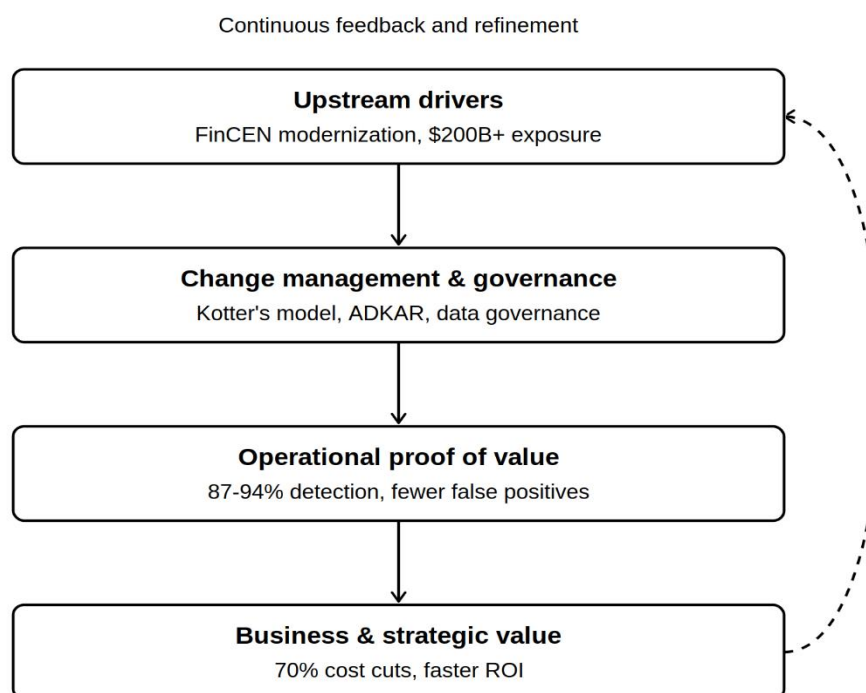
The second major impact dimension is improvements to SAR quality. Automated SAR workflows are more likely to generate more consistent result narratives, have more complete factual documentation, and are closer to FinCEN typology guidance than manually-produced equivalents, according to Sheshadri (2025), because the automated system pulls systematically from the entire SAR transaction and customer record while manual systems are pieced together under time constraints. This improves the intelligence that Law Enforcement can get from SARs, which FinCEN has identified as part of its ongoing effort to modernize SARs. This study by Irfan et al. (2025) demonstrates that the use of AI in financial services compliance leads to tangible improvements in regulatory reporting times, such as a 50–70% decrease in SAR drafting for financial institutions after implementing NLP workflows.

Reducing compliance costs is the most easily measured monetary benefit. Jeyasingh (2023) explains how RegTech implementation in U.S. banking can lead to greater profitability and stability results, lower costs of compliance monitoring, increased accuracy of risk assessment, and a reduced incidence of costly compliance violations and fines for failing to report. In their multi-study review, Bagherifam et al. (2025) discover that RegTech automation can cut compliance processing time by up to 70% and boost accuracy from around 80% to over 95% for institutions that have advanced RegTech implementations. Also, the timeline for realizing the ROI is significantly moderated by the quality of change management: the quality of change management, as indicated by the presence of structured change management programs, influences the timeline for realizing ROI, and those institutions with structured

change management programs see productive system utilization three to six months after deployment, while institutions lacking a structured change management program often report lower than 50% usage of the system capabilities at twelve months (Rafiq & Sohail, 2025). The financial benefits that can be reaped from the investment of fraud reporting automation are also found to be significantly dependent on the organizational and human-side management of the transition, directly supporting the main thrust of this review, which is the benefits of the investment (Karakuş & Yalçın, 2024).

### 3.2 Conceptual Framework

The four thematic domains synthesized in this review are organized into a conceptual framework that maps the entire transformation path of fraud reporting automation within U.S. financial institutions, from the upstream drivers that create the organizational foundation for change, through the change management and governance mechanisms that enable adoption, to the operational improvements and business outcomes that define success. This framework is shown in **Figure 1** and has been developed from the evidence provided in this review.



**Figure 1: An Integrated Framework for Fraud Reporting Automation Transitions in U.S. Financial Institutions (Author's construct, 2026)**

As shown in Figure 1, the automated fraud reporting transformation is not just a technical challenge or solely an organizational challenge for financial institutions in the U.S., but the result of conscious alignment between all four layers of the framework. Upstream drivers create the external pressure for transformation; change management enablers and governance and system design mechanisms create the institutional capability to drive the change; the evidence of value at the operational and compliance level provides the short-term proof of value; and value at the business and institutional level, represented by reduced compliance costs, improved investigator productivity, reduced regulatory risk, and strengthened competitive position, validates the strategic value of the investment after the transformation process. Performance measurement, workforce learning, governance refinement, and system optimization are all outer feedback loops that show that fraud reporting automation isn't a goal, but an ongoing process. Those institutions that embrace it as such, thereby embedding governance and learning structures into the way they operate, not when they go live, are best suited to realize the sustainable fraud reporting excellence represented at its core.

### 4.0 CONCLUSION

This comprehensive review addresses both the technological and human/organizational issues that accompany the shift from conventional manual reporting of fraud to more modern automated reporting systems in financial institutions in the U.S. The evidence presented is clear: adopting automated Suspicious Activity Report (SAR) systems is proven to exponentially increase the accuracy of fraud detection, reduce compliance-related spending, and greatly contribute to the quality of the reports generated. However, this only happens when automated systems are implemented in an environment of structured change management, are supported within a well-defined framework of regulatory alignment, and are backed by an effective data governance framework that is critical to the reliability and effectiveness of automated systems. The most common challenges to the weak implementation of these programs are the lack of coherence on the organizational level, technical deficits and governance issues. Financial institutions

that can successfully apply all four of the lessons and best practices described in this review, in which organizational drivers, change process management, thoughtful system design and measurable impacts are all aligned, will reap the financial benefits and compliance advantages that automation of fraud reporting is supposed to provide. The path to success has been clearly documented and validated, and what really distinguishes the institutions that are successful in this environment is that they follow the organizational discipline required to consistently navigate and follow this path to success.

## REFERENCES

1. Bagherifam, N., Naghdi, S., Ahmadian, V., Fazlzadeh, A., & Baghalzadeh Shishehgharkhaneh, M. (2025). Digital regulatory governance: The role of RegTech and SupTech in transforming financial oversight and administrative capacity. *International Journal of Financial Studies*, 13(4), 217.
2. Berjawi, O., Fenza, G., & Loia, V. (2023). A comprehensive survey of detection and prevention approaches for online radicalization: Identifying gaps and future directions. *IEEE Access*, 11, 120463–120491.
3. Boateng, V., Amoako, E. K., Bonsu, M. A., & Oman-Amoako, M. (2025). Assessing the impact of machine learning model on identifying terrorism financing patterns within the U.S. financial industry. *International Journal for Multidisciplinary Research*, 7(6), Article 62486. <https://www.ijfmr.com/papers/2025/6/62486>
4. Brenner, Z. (2024). Blockchain's Achilles' heel: How interoperability gaps threaten decentralization and invite regulatory scrutiny. *Loyola University Chicago Journal of Regulatory Compliance*, Spring.
5. Cosa, M., & Torelli, R. (2024). Digital transformation and flexible performance management: A systematic literature review of the evolution of performance measurement systems. *Global Journal of Flexible Systems Management*, 25(3), 445–466.
6. Devanga, S. V. (2023). Significance of regulatory technology and its impact on banks and financial institutions amongst the growth of decentralized finance (Master's thesis). National College of Ireland, Dublin.
7. Ferreira, J. J., Cruz, B., Veiga, P. M., & Ribeiro-Soriano, D. (2024). Knowledge strategies and digital technologies maturity: Effects on small business performance. *Entrepreneurship & Regional Development*, 36(1–2), 36–54.
8. Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, & Office of the Comptroller of the Currency. (2025, October 9). *Frequently asked questions regarding suspicious activity reporting requirements*. U.S. Department of the Treasury. <https://www.fincen.gov/system/files/2025-10/SAR-FAQs-October-2025.pdf>
9. Fulford, S. (2026). US consumers' financial exposure to fraud and scams. Available at SSRN 6396678.
10. Irfan, M., Dias, R. T., Hooda, J., Singh, K. A., & Bang, S. (2025). AI's impact on financial services, auditing, and investment strategies: The future ahead. In *AI's transformative impact on finance, auditing, and investment* (pp. 183–224). IGI Global Scientific Publishing.
11. Jeyasingh, B. B. F. (2023). Impact of RegTech on compliance risk due to financial misconduct in the United States banking industry. *Digital Economy and Sustainable Development*, 1(1), 24.
12. Karakuş, M., & Yalçın, C. (2024). Digital transformation and organizational change management: Theoretical models and case studies. *New Trends and Frontiers in Engineering*, 344–376.
13. Oyekunle, S. M., Popoola, A. D., Kolo, F. H. O., Ogunmolu, A. M., & Adesokan-Imran, T. O. (2025). Intelligent fraud prevention information banking: A data governance-centric approach using behavioural biometrics. *Asian Journal of Research in Computer Science*, 18(5), 525–543.
14. Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155–166.
15. Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*, 33(1), 37.
16. Rafiq, M., & Sohail, M. K. (2025). Adopting regulatory technology for anti-money laundering in banking: Key enablers and barriers in a RegTech model. *Sustainable Futures*, 10, 101377.
17. Reports by Banks of Suspicious Transactions, 31 C.F.R. § 1020.320 (2024). <https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-C/section-1020.320>
18. Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI driven fraud detection models in financial networks: A review. *IEEE Access*, 13, 141204–141233.
19. Sheshadri, K. (2025). Analysis on importance and effectiveness of suspicious activity reporting (SAR) for the anti-money laundering process of investment banks in India (Master's thesis). National College of Ireland, Dublin.
20. Tucker, O. (2024). Risk-based customer due diligence is the key to effectively managing financial crime risk. *Journal of Financial Compliance*, 8(1), 65–79.