Sarcouncil Journal of Economics and Business Management

ISSN(Online): 2945-3593

Volume- 05| Issue- 04| 2026

Research Article **Received**: 25-02-2026 | **Accepted**: 20-03-2026 | **Published**: 07-04-2026

Role of Artificial Intelligence in Enhancing Suspicious Activity Reporting (Sar) for U.S Financial Institutions

Tosin Oladokun[1], Clement Abugri[2] and Yeboah Mary Magdalene[3]

[1]*University of Carlifornia, Berkeley, Haas School of Business, Berkeley, CA*
[2]*University of Texas at Dallas-Dallas, Texas*
[3]*University of Ghana, Legon*

Abstract: Suspicious Activity Reports (SARs) serve as a fundamental tool in identifying and addressing financial crimes such as money laundering, fraud, and terrorist financing within U.S. financial institutions. As globalization and transaction complexity increase, traditional methods often fall short in adapting to evolving fraud patterns, leading to substantial financial losses for institutions and customers, while also eroding consumer trust. This paper explores how Artificial Intelligence (AI), particularly machine learning and natural language processing, enhances SAR effectiveness by improving detection accuracy, enabling real-time monitoring, and automating narrative generation. Under the regulatory framework of the Bank Secrecy Act (BSA), AI technologies empower institutions to meet compliance standards while reducing operational costs and false positives. However, challenges such as model explainability, data quality constraints, algorithmic bias, and the persistence of false-positive alerts highlight the limitations of AI-driven systems and the need for robust governance and human oversight. Case studies from JPMorgan Chase, HSBC, and Bank of America illustrate both the transformative potential and practical constraints of AI in fraud detection, SAR quality, and customer experience. The findings underscore AI's role in revolutionizing financial compliance while emphasizing the importance of balancing innovation with transparency, accountability, and regulatory alignment.

Keywords: Suspicious Activity Reporting, Artificial Intelligence, Machine Learning, Natural Language Processing, Bank Secrecy Act.

INTRODUCTION

Suspicious Activity Reporting (SAR) is a critical process used by financial institutions to help detect and prevent financial crimes such as money laundering, fraud, and terrorist financing. According to FinCEN (2024), SARs serve as a foundational tool in maintaining financial integrity and national security. Money laundering, the process of concealing illegally obtained funds to make them appear legitimate, poses a significant threat.

Due to rapid globalization and increasingly complex financial transactions, the U.S. financial system faces increasing threats from illicit activities. As money launderers adopt more advanced techniques, the detection and prevention of financial crimes have become critically important. Financial institutions play a crucial role in combating financial crime through their compliance with the Bank Secrecy Act (BSA), a legislative framework enacted in 1970 to prevent the misuse of the banking system for illicit purposes (Bradstreet, 2019).

The Suspicious Activity Reporting system (SARs), created by the five federal financial supervisory agencies and the Financial Crimes Enforcement Network (FinCEN), is a tool provided under the Bank Secrecy Act (BSA) of 1970 for monitoring suspicious activities or illegal financial transactions that are deemed out of the ordinary (Kenton, 2024; FDIC, 2017). However, the global shift towards digital payments, e-commerce, and online banking has further accentuated the need for robust fraud detection systems (Smith, J., & Jacob, R. 2024). Traditional SAR processes often suffer from delays, inaccuracies, and resource constraints, limiting their effectiveness in a fast-paced financial environment.

In response to this challenge, Artificial Intelligence (AI) plays a vital role in enhancing SAR capabilities. Advanced AI algorithms can cross-reference vast amounts of structured and unstructured data from multiple sources, identifying patterns indicative of financial misconduct, such as money laundering, terrorist financing, or fraudulent asset transfers with high accuracy, speed and consistency, revolutionizing compliance and strengthening the fight against financial crime (Adejumo & Ogburie, 2025; Fauzia, A.Clottey, 2025).

This paper examines the role of Artificial Intelligence in improving Suspicious Activity Reporting systems. It first explores the limitations of traditional SAR processes, then analyzes how AI-driven approaches enhance detection and reporting efficiency and finally discusses the

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Tosin Oladokun

DOI-https://doi.org/10.5281/zenodo.19451863

challenges and future implications of integrating AI into financial crime prevention frameworks.

BACKGROUND AND REGULATORY FRAMEWORK.

The BSA refers to a set of laws and regulations enacted in the United States to combat money laundering and the financing of terrorism (FDIC, 2017). The Bank Secrecy Act of 1970, passed by Congress, was designed to prevent criminals from concealing or laundering illicit gains through the U.S. banking system. The statute requires financial institutions to maintain currency transaction reports and identify individuals conducting suspicious transactions (Bradstreet, 2019).

Under this law, the Department of the Treasury is authorized to impose reporting and other requirements on financial institutions and businesses to help detect and prevent illicit activities, such as money laundering, tax evasion, and other criminal conduct. The BSA mandates that U.S. financial institutions assist law enforcement agencies by maintaining appropriate records and filing reports of suspicious activity within 30 calendar days of detection, typically through the BSA E-Filing System (FinCEN, 2024; U.S. Government Accountability Office, 2009; Fauzia, A.Clottey, 2024). The Financial Crimes Enforcement Network (FinCEN) is responsible for implementing, administering, and enforcing BSA regulations.

However, the traditional Suspicious Activity Reporting (SAR) process is resource-intensive and prone to errors. To address these challenges, financial institutions are increasingly leveraging artificial intelligence (AI) to enhance compliance efforts and reduce operational burdens.

ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN SAR ENHANCEMENT

According to Gerlings and Constantiou (2023), AI has significantly enhanced the generation and quality of Suspicious Activity Reports (SARs) particularly machine learning for transaction monitoring**.** Improved detection accuracy machine learning models are now enabling financial institutions to sift through vast and complex transactions with ease. AI uses different learning methods to detect suspicious transactions: supervised learning, unsupervised learning and reinforcement learning. By analyzing large volumes of complex data, these advanced systems make it easier to detect unusual activity earlier that might otherwise go unnoticed by human analysts or rule-based systems for further investigation.

Moreover, AI's real-time processing capabilities allow institutions to monitor transactions as they occur**.** In a landscape where speed is just as important as accuracy, the ability to monitor voluminous transactions as they happen and instantly flag suspicious behavior is a game-changer. This not only enhances compliance efforts but also enables institutions to intervene sooner, limit potential losses and preserve evidence trails.

Additionally, AI technologies, particularly Natural Language Processing (NLP), play a crucial role in generating clear and compliant narratives Suspicious Activity Reports (SARs), as required under the Bank Secrecy Act (BSA) and enforced by FinCEN (Financial Crimes Enforcement Network). NLP tools help automate the drafting of more coherent and accurate SAR narratives, improving report quality. This helps compliance teams to save significant time and resources.

BENEFITS OF USING AI FOR SARS

According to Adejumo & Ogburie (2025), AI offers numerous benefits in enhancing SAR detection and compliance within U.S. financial institutions. Machine learning models improve precision in transaction monitoring by analyzing voluminous transactions to detect patterns with greater confidence and compliance that traditional rule-based systems often miss, and these models learn from historical SAR data as well as adapting to new fraud patterns as they emerge, which helps to reduce false positives.

Additionally**,** AI technologies act as alert triage systems for financial institutions, streamlining the detection of illicit financial activities and helping prevent financial losses. This enhances operational cost efficiency.

Natural Language Processing (NLP) tools further enhance SAR quality by generating **clear, concise,** and regulation-compliant narratives, **making it easier for regulators to compare and analyze cases, as well as to track illicit financial activities.**

REAL-WORLD APPLICATIONS AND CASE STUDIES.

JPMorgan Chase: Real-time fraud prevention.

JPMorgan Chase, a leading global financial services firm, employs advanced AI technologies to combat fraud and manage risk. Leveraging

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

machine learning and anomaly detection, JPMorgan Chase enhances security and protects its customers and assets. This case study examines how JPMorgan Chase utilizes AI to safeguard its operations and maintain financial integrity (GetEasy.ai 2025; Fauzia, A.Clottey,2025). JPMorgan Chase needed a more efficient way to detect and respond to fraudulent transactions in real time. Traditional systems produced too many false positives, increasing the workload for compliance teams and delaying response times**.**

To overcome this significant challenge, JPMorgan implemented AI technology in fraud prevention for more than two years. This strategic shift yielded significant improvements across many aspects of the bank's operations. One of the most notable outcomes was the reduction in false positives by over 50%, and improved customer experience, with account validation rejection rates cut by 15-20%.

In addition to accurate improvements, JPMorgan saw gains in how effectively alerts were managed. With the integration of Promon's AI technology, the bank was able to improve alert prioritization by 25%, which helps compliance teams work smarter, not harder and streamlined the manual review process, significantly reducing the compliance team's workload (J.P. Morgan,2023)

HSBC: Improving detection using AI.

Historically, HSBC faced challenges with high false positive rates and inefficient detection of financial illicit activities using its legacy rule-based Anti-Money Laundering (AML) system**,** which not only overwhelmed compliance teams but also diluted the effectiveness of its monitoring efforts. The rule-based system, while rigid, lacked flexibility to adapt and precision needed to identify more complex illicit financial activities.

To address these challenges, HSBC implemented an internal AI-driven system known as Dynamic Risk Assessment, to enhance its Anti-Money Laundering (AML) efforts and improve risk evaluation processes. The result of this implementation is substantial. Compared to the legacy system, the new AI-powered approach was able to detect accuracy by finding two to four times more financial crime than its legacy rule-based systems. Moreover, it achieved a 40% reduction in false positives, allowing teams to concentrate on genuinely high-risk cases.

Beyond improving accuracy, the Dynamic Risk Assessment system significantly enhanced detection capabilities by shortening the time needed to process billions of transactions across millions of accounts from weeks to just a few days. This allowed HSBC to identify indicators of financial crime more swiftly and minimize the impact on customers and supplying law enforcement with more valuable information, which leads to better results in combating financial crime (Calvery, J. 2024)**.**

Bank of America: Using AI in Fraud Prevention

Bank of America believes every account is at risk for fraud. Therefore, it has established a sustainable cybersecurity program grounded in accountability, consistency, measurement, and a strict code of ethics requiring all employees to maintain the confidential treatment of client information. As banking evolves, AI is transforming how banks operate, connect with customers, and maintain security. Bank of America stands out as a leader by strategically integrating AI across multiple facets of its business, thereby enhancing efficiency, customer experience, and security.

The bank has implemented generative AI across its digital platforms to improve customer service by providing real-time, customized interactions that deliver immediate responses to customer inquiries and generate proactive insights, helping customers make informed financial decisions.

Additionally, it utilizes machine learning algorithms trained on historical transaction data to detect unusual patterns and potential fraud. This approach has resulted in a reduction in fraudulent transactions, along with increased customer satisfaction and security (Bank of America, 2024)

CONCLUSION

As financial crimes grow more sophisticated and globalized, the shortcomings of traditional Suspicious Activity Reporting (SAR) systems are becoming more noticeable than ever. This paper demonstrates that Artificial Intelligence (AI), particularly machine learning and natural language processing, can effectively address these issues. AI enhances transaction monitoring in real time, improves detection accuracy, and streamlines SAR narrative creation, leading to greater efficiency, accuracy, and compliance.

Incorporating AI within the regulatory framework of the Bank Secrecy Act (BSA) enhances

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

institutional robustness while simultaneously lowering compliance costs and minimizing the rate of false positives., allowing compliance teams to focus on genuinely high-risk cases. Case studies from JPMorgan Chase, HSBC, and Bank of America show compelling evidence of AI's practical impact, from fraud prevention and alert prioritization to improved customer experience and faster investigative turnaround.

Ultimately, the adoption of AI in SAR processes marks a pivotal shift in how financial institutions combat illicit activities. As these technologies continue to evolve, they will play an increasingly vital role in safeguarding financial systems, restoring consumer trust, and supporting law enforcement efforts in the fight against financial crime.

REFERENCES

1. Paul, A. A., & Ogburie, C**.** "The Role of AI in preventing financial fraud and enhancing compliance." *GSC Advanced Research and Reviews* 22.3 (2025): 269-282.
2. United States Government Accountability Office (GAO), **"**Bank Secrecy Act: Suspicious Activity Report Use Is Increasing, but FinCEN Needs to Further Develop and Document Its Form Revision Process **(**2009**).**
3. Bradstreet, S. M. "REFORMING THE BANK SECRECY ACT TO ADDRESS EMERGING TECHNOLOGY AND PREVENT ILLICIT FINANCING." Diss. Monterey, CA; Naval Postgraduate School, (2019).
4. FDIC. "The Bank Secrecy Act: A Supervisory Update. Supervisory Insights," *Summer*.2017**.** (2017).
5. Smith, J., & Jacob, R. "Fraud Detection in Financial Transactions Using Deep Machine Learning." (2024).
6. Gerlings, J., & Constantiou, I. "Machine learning in transaction monitoring: The prospect of xai." *arXiv preprint arXiv:2210.07648* (2022).
7. Abilash, A., Suresh, D., Yamini, B., Maheswari, B., & Gracious, L. A. "AI in Risk Management: An Overview of Applications in Firm Management, Financial Markets, and Risk." *Artificial Intelligence for Financial Risk Management and Analysis* (2025): 455-470.
8. JMorgan, J. P. "How AI will make payments more efficient and reduce fraud." (2023),
9. Fauzia, A. Clottey. "An Integrated Operations–Leadership Framework For Enhancing Supply Chain Efficiency And Financial Oversight." *IPHO-Journal of Advance Research in Applied Science* 3.12 (2025): 42-49
10. GetEasy.ai.. "JPMorgan Chase: AI for Fraud Detection and Risk Management." *Retrieved from GetEasy.ai case* (2025).
11. Calvery, J. "Harnessing the power of AI to fight financial crime." *HSBC, available at: Link to the cited article* (2024).
12. Kenton, W. "What Is a Suspicious Activity Report (SAR)? Triggers and Filing." Investopedia. (2024).
13. Fauzia, A. Clottey. "Optimizing Business Growth Through Strategic Leadership: Evidence From Team Development, Supply Chain Management, And Operational Efficiency." *IPHO-Journal of Advance Research in Business Management and Accounting* 2.11 (2024): 32-39
14. Fauzia, A. Clottey. "The Role of Strategic Leadership in Strengthening Team Performance and Supply Chain Resilience for Business Growth." *IPHO-Journal of Advance Research in Business Management and Accounting* 3.07 (2025): 16-23
15. FinCEN. "Suspicious Activity Reports (SARs): Definition and Filing Process." *Finance Strategists.* (2024).
16. Bank of America. "Using machine learning and generative AI to transform fraud prevention and customer experience." *Business Insights on AI and Cybersecurity*. (2024).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Oladokun, T., Abugri, C. & Magdalene, Y. M. "Role of Artificial Intelligence in Enhancing Suspicious Activity Reporting (Sar) for U.S Financial Institutions." *Sarcouncil Journal of Economics and Business Management* 5.4 (2026): pp 1-4.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher