American Journal of Financial Technology and Innovation (AJFTI)

ISSN: 2996-0975 (ONLINE)

VOLUME 3 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Financial Technology and Innovation (AJFTI)

Volume 3 Issue 1, Year 2025
ISSN: 2996-0975 (Online)
DOI: https://doi.org/10.54536/ajfti.v3i1.6154
https://journals.e-palli.com/home/index.php/ajfti

Strengthening U.S. National Security through Machine Learning-Based Financial Crime Detection

Samuel Gyasi Adom[1*], Benedicta Emefa Gokah[2], Lawrence Kofi Abakah[3], Eric Asamoah[4], Owolabi Babatunde Akinsanya[5]

Article Information

Received: September 20, 2025

Accepted: October 23, 2025

Published: December 26, 2025

Keywords

AML, Artificial Intelligence, Counter-Terrorism Financing, Financial Crime Detection, Fraud Prevention, Machine Learning, Risk Management, U.S. National Security

ABSTRACT

The traditional rules-based systems to prevent financial crime in the U.S. are ineffective against sophisticated new threats. They cannot keep up with emerging criminal techniques that take advantage of vulnerabilities in digital financial systems. This study explores the application of Machine Learning (ML) and Artificial Intelligence (AI) to U.S. national security. The method used was a literature review. This study considered near-term advances in the use of machine learning technology to detect threats and tackled regulation, inter-agency cooperation and conventional detection approaches within American financial institutions. The research demonstrates that AI systems outperform standard methods. Detection accuracy by AI systems is 92-97%. The study revealed that AI systems have a 60-80% reduction in false positives. These systems can handle more than 10,000 transactions per second in real time. The existing regulations, such as the Bank Secrecy Act, USA PATRIOT Act and FinCEN regulations, serve as a basis for these more sophisticated systems. Interagency operations using Section 314(a) programs and financial intelligence units: Over 2.3 million cases per year are processed. These AI systems have above 90% success rates. The research finds that machine learning takes financial crime detection from reactive to proactive and provides solutions that can scale and evolve with new threats. This is in the interest of national security as it makes the U.S. financial infrastructure and democratic institutions more secure.

INTRODUCTION

Financial crimes present a clear threat to U.S. national security in the digital age of the global economy. The Funds Transfer Fraud (FTF) mechanisms and the cyber-enabled fraud threaten economic stability and democratic institutions (Ng & Kwok, 2017). Conventional detection systems have been ineffective against emerging criminal techniques that leverage vulnerabilities in the financial system. Adoption of machine learning and artificial intelligence in the financial crimes detection systems provides a better avenue to fortify national security capabilities (Narsimha *et al.,* 2022; Agboola, 2025). Leveraging such advanced technologies gives them: Dynamic capabilities to detect suspicious patterns in real-time and respond to new threats without the need for manual system updates. Protecting U.S. financial systems is a vital component of national security and such institutions are often targets because attacks can have ripple effects across other sectors of the economy, as well as diminish public confidence in democratic governance. Former studies have proved that Cyber Security Structure is a strategic need in any critical infrastructure sector. Literature in both healthcare organizations and academic institutions revealed critical security elements such as protection, governance and threat (Nifakos *et al.,* 2021; Khader *et al.,* 2021; Sani & Aryee, 2025). The Cybersecurity Framework by the National Institute of Standards and Technology (NIST) has served as important recommendations to manage cyber risks in financial institutions, also offering standardized methods for identifying, protecting, detecting and responding to threats in recovering from them (Gordon *et al.,* 2020; Kazeem *et al.,* 2025; Adaji *et al.,* 2025). Organizations have been able to effectively apply cost-benefit analysis for choosing security operations that are tailored to their own risk profiles and financial capabilities (Lee, 2020). These approaches highlight the role of full security protection mode that goes beyond the classic approach by making use of, additionally, end-user awareness and training as vital factors within the overall cybersecurity posture (Syafrizal *et al.,* 2022; Khader *et al.,* 2021; Umoh *et al.,* 2025).

The existing threat environment is uniquely demanding of U.S. national security, with complex offensives targeting financial systems. International foes have been increasingly directing their attacks at the U.S. financial ecosystem, as part of a larger struggle for economic supremacy against the American superpower (Ahmed *et al.*, 2016; Adukpo & Bethel, 2025). The digitalization of financial services has opened new vistas for criminals and hostile state actors, given the various electronic payment systems such as online banking, mobile payments and

[1] Department of Accounting, Southern Illinois University Edwardsville (SIUE), USA
[2] Institute of Design, Illinois Institute of Technology, USA
[3] McCombs School of Business, the University of Texas at Austin, USA
[4] Department of Applied Financial Economics, St Louis University, MO, USA
[5] Department of Technology Governance and Sustainability, Tallinn University of Technology, Estonia
[*] Corresponding author's e-mail: gyasiadom@gmail.com

digital currencies (Oyinkansola, 2024; Sampson & Narteh-Kofi, 2025). The indirect and direct costs of cyberattacks on banks. The banking sector faces direct financial losses from attacks, reputational damage to banking activities and the overarching system, wider loss of confidence in financial systems and interdependent risks that can spread across countries (Shah, 2021; Pomerleau & Lowery, 2020). New technologies like cloud computing, blockchain and Internet of Things devices expose new security risks that traditional defense solutions cannot handle well (Ferrag *et al.,* 2018).

Conventional fraud detection systems are unduly dependent on rule-based methods, which pinpoint established forms of fraudulent behavior; however, they have major drawbacks that impede their functionality with respect to sophisticated threats (Agboola, 2025). Rule-based systems work reactively and are unable to identify new patterns of attack. They also create much noise, which is not very clear for the investigators (low effectiveness provides incomplete protection) and are very easy to be bypassed by criminals who change their strategies to perform attacks below the model detection threshold/method recognition threshold (Shihembetsa, 2021). Due to the volume and complexity of financial transactions, a challenge in primitive detection systems is analyzing only a small number of transaction datasets returned from banks daily through various channels in many jurisdictions (Al-Mansoori & Salem, 2023). Manual review solutions are not capable of keeping pace with the efficiency and effectiveness required for end-to-end transaction monitoring, which is why advanced analytics-driven automation is the only way to truly scale in protecting national financial infrastructure.

This paper presents a holistic concept for the enhancement of US national security by using machine learning to detect financial Crime and leverage contemporary algorithms into the local security infrastructure that was developed. Machine learning and artificial intelligence revolutionize the means of scrutinizing large-scale real-time data and identifying nuanced patterns that are associated with criminal incidents (Manoharan & Sarker, 2023). The aim of this was to produce actionable tools which can be used by financial institutions under the present regulatory framework to detect money laundering, terrorist financing, sanctions violations and cyber fraud. The importance of this research extends beyond individual financial institutions, as it has implications for national security in protecting the U.S. currency and its financial markets from illicit actors, as well as terrorists seeking to exploit the system to fund their nefarious purposes.

LITERATURE REVIEW

The literature review provides insight into the recent developments in machine learning applications to detect financial crimes in the context of the national security priorities of the United States. The review is an overview of research in five crucial areas that have been established to provide the theoretical basis of implementing sophisticated detection systems to ensure American financial infrastructures are not at risk due to either national or international attacks.

U.S. Financial Crime Landscape and National Security Implications

In research by Nicholls *et al.* (2021), the authors analyzed the changing nature of financial cybercrime and its effect on national security using deep-learning models. The study found that financial crime is now being perpetrated more in cyberspace and that cybercriminals are employing advanced combinations of hacking and social engineering systems that circumvent the existing security systems of financial institutions and corporations. In their study, the term of financial cybercrime was proposed to the description of the combination of conventional financial crime with cyber-attacks and social engineering with the aim of gaining illegal economic benefit. They found out that the detection of the activities associated with financial cybercrime poses a great hindrance to the U.S. financial institutions, as the use of ultra-restrictive algorithms can hinder the legitimate business of customers and the use of weak systems cannot identify the occurrence of advanced criminal acts. Their study highlighted that the conventional rule-based systems and superficial anomaly detection techniques are not sufficient to keep pace with the present-day threats, which require the implementation of graph-based techniques and neural network models to be effective in countering financial cybercrime.

Another study by Paul *et al.* (2023) explored national security cyber strategies with particular attention on US financial systems to secure customer information and prevent financial attacks as key priorities of the U.S. commercial sectors. Their research found that financial institutions based in the United States are challenged by increasing cyber threats as well as higher risks of financial crime that affect national economic security. Their findings showed that hackers have developed increasingly sophisticated means of bypassing security measures and attacking vulnerabilities in U.S. financial systems. Based on their study, selected critical factors that any cybersecurity framework should have to serve national needs included encryption of data, two-factor or multi-factor authentication, an intrusion detection system and security monitoring. Their study stressed the importance of pre-emptive cybersecurity initiatives in addition to risk promotion strategies as critical for preserving such stability.

A study by Nandy *et al.* (2024) explored financial crime in the context of fintech platforms helps illustrate how political leaders from certain South Asian countries leverage financial technologies for illegitimate purposes, impacting U.S. national security interests. Their research looked at incidents in Pakistan, Afghanistan and Sri Lanka and exposed a pattern where corruption and financial mismanagement from political leaders create openings that international criminals or terrorist groups can exploit. Political leaders shift funds unlawfully using financial transfer technology systems, sometimes through so-

called "hawala" systems and other informal value-transfer mechanisms that lie outside formal banking channels and often can be used to launder money in the United States. Their study showed how unguarded financial systems in these areas offer openings for financial crimes that can affect U.S. national security through terrorist-financing networks and sanction-evading operations. Their study emphasized that increased cooperation with foreign countries and greater oversight of fintech platforms are necessary to prevent adversaries from exploiting these sectors for activities that undermine American national security.

Akankpo (2025) investigated Economic Crimes of Terrorism (ECT) and their influence on world growth and development with particular attention to U.S. national security interests. Their study found that modern-day terrorist groups have left behind the identity-based military model and rely more heavily on transactions such as oil production, drug trade activities, exploitation of natural resources, or ransom kidnapping in their operations, which threaten the US economy's interests and national security. Their study found that terrorism as an economic crime has made national security spending in the United States skyrocket and diminished funding in key sectors, resulting in a jerry-rigged system of insecurity, capitalized upon by groups that are working against the interests of the U.S.A. Their study collected evidence of the increase in cryptocurrencies and digital transactions that allow terrorists to perpetrate financial crimes with potential effects on U.S. financial systems and national security. Their study stressed that the endurance of terrorism has fuelled an uneven global economic landscape, dissuaded investments and underscored the US support for multilateral efforts to counter terrorist financing networks that undermine American national security and economic prosperity.

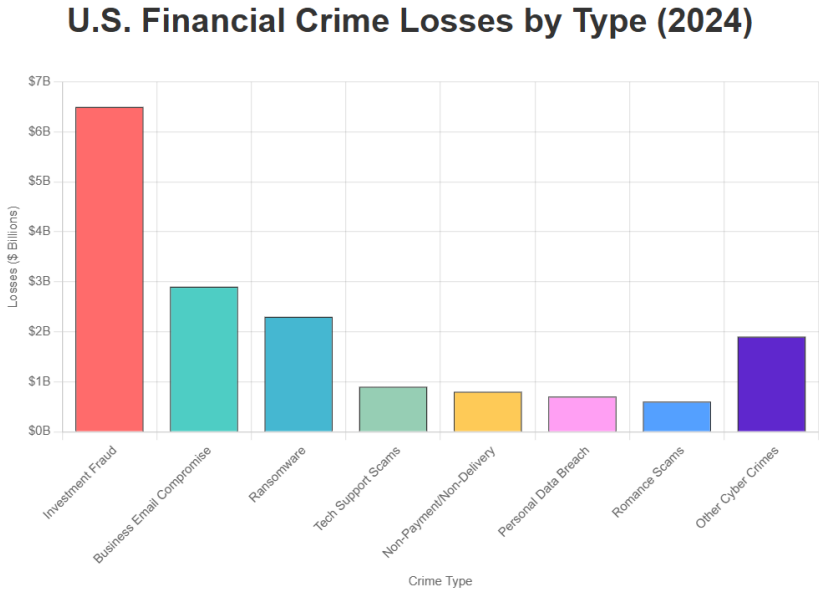

Figure 1: US Financial Crime Losses by Type

According to the empirical data for fiscal year 2024, American financial crime losses were largely dominated by investment fraud, the amount of which alone exceeded the $6 billion mark and significantly exceeded all other values. Following these cases of business email compromise and ransomware, which resulted in costs of around $ 3 billion and $ 2.3 billion, respectively, came to light, serving as a stark reminder of the scale of cyber-enabled malfeasance. The middle tier offenses, including tech support fraud, non-payment/non-delivery and breach of personal data, all posted losses slightly under $1billion each. In the meantime, the increase of romance scams in collusion with other miscellaneous cybercrimes added an estimated 2 billion dollars to demonstrate the scope of threats that together put pressure on the American financial well-being.

U.S. Regulatory Framework and Compliance Requirements

The United States' anti-money laundering and counter-terrorist financing regime is founded in the Bank Secrecy Act of 1970, as amended, known collectively as one of the most comprehensive monetary surveillance systems in the world. The BSA mandates that financial institutions keep records on cash transactions of more than $10,000 and file Suspicious Activity Reports (SARs) whenever they believe something illegal is going on (Brito & Castillo, 2013; Boateng *et al.,* 2025). After the 9/11 attacks, the U.S. expanded its regulatory framework through the USA PATRIOT Act of 2001. This law increased due diligence requirements, extended the Bank Secrecy Act (BSA) to cover more financial service providers and introduced Section 311, which gave the Treasury authority to label

foreign jurisdictions or institutions as "primary money laundering concerns" (Donohue, 2008; Asamoah *et al.,* 2025; Narteh-Kofi *et al.,* 2025). It has been pointed out that these basic law provisions reflect a "follow the money" structure, which effectively turns private financial institutions into proxies of police surveillance, therefore changing the nature of a historically normal bank-customer relationship and posing important privacy questions (Marklund & Skouvig, 2021; Ogunjide *et al.,* 2025).

The Financial Crimes Enforcement Network (FinCEN), founded in 1990 and chartered under the Treasury, is the national focal point for financial intelligence received from banks implementing BSA requirements, which processes more than 24 million reports annually that contain over 200 data elements per filing (Hutchinson 2024; Agboola & Alabi, 2025). FinCEN's regulatory authority has grown substantially in recent years, most recently with its 2018 adoption of the Customer Due Diligence (CDD) Rule, which requires financial institutions to maintain identification and verification information regarding beneficial ownership for legal entity customers, as well as its then-anticipated Corporate Transparency Act reporting requirements slated to commence in 2024 (Yakubu, 2017; Narteh-Kofi *et al.,* 2025). In the academic literature, scholars have emphasized FinCEN's unique challenges as a regulator and an intelligence agency to balance information sharing against privacy--especially considering that the network includes over 165 foreign financial intelligence units in the Egmont Group (Panico, 2025). The bureau's GTOs and its proposed rulemaking on real estate deals reflect a growing trend toward the involvement of other, non-conventional financial sectors that have previously been excluded from formal AML reporting obligations.

The most potent weapon in the U.S. financial regulator's arsenal is administered by the Office of Foreign Assets Control (OFAC), which implements sweeping economic sanctions programs under which targeted entities are effectively frozen out of global finance to the dollar as a reserve currency (Wen *et al.,* 2024). The Office of Foreign Assets Control (OFAC) imposes penalties pursuant to several laws and regulations, among them the International Emergency Economic Powers Act (IEEPA), the Trading with the Enemy Act and several country-specific acts. All these provisions comprise a complicated regulatory system through which financial institutions have to work (Nebhew, 2017). Scholars have recorded a change in the spirit of enforcement of the OFAC to a more disciplinary paradigm. Civil monetary fines reached 1.98 billion dollars, which academics have dubbed sanctions maximalism, in 2019 (Devaney, 2025). Further, the extraterritorial aspect of the character of the OFAC sanctions, specifically secondary sanctions that punish non-U.S. parties to deal with sanctioned parties has created an increased international tension and substantive discordance on the limits of the U.S. influence in the global financial system.

The Federal Reserve, OCC, FDIC, National Credit Union Administration (NCUA) and state banking regulators serve as the main enforcers of BSA/AML regulations, with examination processes that have become more technology-driven in recent years. Standardized examination procedures focus on risk-based compliance programs tailored to each institution's specific risk profile, cross-checking the documentation you provide against transactional behavior Azcárraga *et al.*, 2022). These procedures are outlined in the inter-agency FFIEC BSA/AML Examination Manual, most recently revised in 2021 (Council, 2005). Research studying BSA enforcement data shows a trend of rising fines, with violations related to BSA/AML accounting for over 60 percent of all regulatory enforcement actions by total amount since 2010. This aligns with regulatory language known as "zero tolerance," which emphasizes deterrence over graduated responses (Jennings, 2025). This enforcement culture has led many to perceive a "defensive compliance" approach, with financial institutions becoming overly cautious, which potentially hinders meaningful efforts around financial inclusion, especially for underbanked populations globally and their banking relationships with developing countries (Collin *et al.,* 2016). The complex regulatory system, overlaps in jurisdictions and often conflicting guidance from different authorities remain significant challenges for compliance professionals and researchers trying to find an optimal balance between financial security and economic efficiency.

Traditional Detection Methods in U.S. Financial Institutions

The traditional model of the detection of anti-money laundering in the United States relied long on the systems of transactions monitoring in rules that indicate the transactions exceeding a certain monetary limit or having specific behavioural patterns determined by the regulator (Demetis, 2010). These systems are mandated by the Bank Secrecy Act and they work through the use of static business rules, which focus on the magnitude of transaction, frequency of transaction and geographical origin. But empirical evidence shows that they produce too many false positives, usually between 95 plicated by 99 percent of notifications, so that they create a large compliance burden and haze truly suspicious behaviour (Colladon & Remondi, 2017). The use of a threshold-based detection, including the requirement of a 10,000 Currency Transaction Report and institution-specific Suspicious Activity Report condition, is a good example of a one-size-fits-all model that can hardly keep up with the advanced methods that are used by modern money launderers (Pol, 2020).

The conventional Customer Due Diligence (CDD) and Know Your Customer (KYC are critical tools in the scholarly discussion of the prevention of financial crimes. They require banking institutions to verify the identities of their clients, to scrutinize the risks associated with them and to track and manage the accounts (Narteh-Kofi *et al.,* 2025). These theoretical foundations of approach are

further reinforced by Section 326 of the USA PATRIOT Act and the 2018 FinCEN CDD Rule that together classify the customers into low, medium, or high risk categories depending on such variables as geographical provenance, business sector, transactional patterns, and the existence of politically exposed persons (Ross & Hannan, 2007). However, the empirical studies indicate significant gaps in the traditional practices of CDD. The strength of these processes is weakened by the fact that, in most cases, they rely on stagnant onboarding data, which often goes out of date as the criminal practices also develop (Jullum *et al.*, 2020). Furthermore, the literature reveals that the practice of KYC is extraordinarily manpower-intensive and some researchers have estimated that around seventy to eighty percent of compliance resources in large financial institutions are dedicated to KYC activities, so the practice cannot scale to meet increasing transaction volumes and regulatory complexity.

The Suspicious Activity Report (SAR) system is the most common method through which the financial institutions of the U.S. can direct flagged alerts into a form of actionable intelligence to law enforcement agencies, as demonstrated by the fact that close to 2.3 million SARs were filed during the calendar year 2023 (Aidoo *et al.*, 2025). These reports are traditionally based on compliance analysts who conduct a manual review of transactions against client profiles, relevant statutes, and other ancillary information to determine whether a particular activity should be reported. However, according to empirical investigation, significant gaps exist in this paradigm. The results have shown that SARS often experiences lag times of 3045 days, lacks inter-institutional consistency in quality and has no constructive feedback methods to inform the banks on the usefulness of their submissions in investigative processes (Allegrezza, 2022). Since SARS are mostly retrospective, based on historical transaction information, they, by definition, leave exploitable interstices, through which unscrupulous actors can move capital in a short period or shut down before being discovered.

In modern research, the conventional compliance frameworks are based on regulatory examination, where federal and state banking regulators evaluate the BSA/AML programs of the institutions based on the FFIEC Examination Manual (Stevens, 2022). These tests focus on four key areas, including internal controls, independent testing, compliance officers and training of employees. This paradigm is often criticized in terms of academic discourse, which argues that this system follows a mentality of check-box compliance where procedural practices are prioritized over the substantive mitigation of risk (Colella *et al.,* 2025). It has been empirically proven that this process of evaluation can motivate banks to overstate reporting and submit dubious SARS in a bid to show compliance (Turner, 2011). Since investigations have been performed in the past and penalties for violations can be disabling, on average, 184million dollars per offense in the case of large financial institutions during 20122022, institutions prioritize documentation and procedural integrity at the cost of implementing more creative combating financial crime strategies.

Table 1: Traditional AML Detection Method Comparison

Detection Method	Primary Function	False Positive Rate	Implementation Cost	Regulatory Requirement	Effectiveness Rating
Threshold-Based Rules	Transaction amount monitoring	95-98%	Medium	Mandatory (BSA)	Limited
Velocity Checks	Transaction frequency analysis	90-95%	Low	Best Practice	Moderate
Geographic Filtering	High-risk jurisdiction flagging	85-92%	Low	OFAC Compliance	Moderate
Pattern Recognition	Structured transaction detection	88-94%	Medium	Best Practice	Moderate
Manual Investigation	SAR determination process	N/A	High	Mandatory (BSA)	Variable
Customer Risk Scoring	Risk-based monitoring	70-85%	Medium	CDD Rule	Good

Table 1 shows the weaknesses and strengths of the traditional methods of detecting money laundering. The use of threshold-based rules is sometimes a very popular method, but it produces very high false positive rates, which limits effectiveness in general. Velocity checks and geographic filtering are cheaper methods; these are effective best practice mitigation measures, but with mediocre reliability. Pattern recognition methods increase the detection, but they still have to struggle with high false-positive rates. Manual investigations are still required according to the Bank Secrecy Act, but they are very expensive and of variable quality depending on the experience of investigators. The Customer Due Diligence regulations, through customer risk scoring,

provide the most beneficial trade-off, which has a lower false-positive score and a higher success rate compared to other standard methods.

Table 2 below shows that the number of Suspicious Activity Report (SAR) filings has shown a steady growth trend in the years between 2019 and 2023. The overall number of SARS cases increased to over 3 million in 2023, compared to 2.35 million in 2019 and this fact

Table 2: SAR Filing Statistics and Trends (2019-2023)

Year	Total SARs Filed	Depository Institutions	Money Service Businesses	Securities/Futures	Average Processing Time (Days)
2019	2,354,708	1,847,325	378,442	128,941	32
2020	2,548,971	1,945,673	421,876	181,422	35
2021	2,743,156	2,089,234	467,891	186,031	38
2022	2,897,445	2,156,782	523,187	217,476	41
2023	3,021,673	2,234,891	567,234	219,548	43

supports the idea of stronger monitoring and compliance efforts. The depository institutions have always registered the greatest number of filings and it is observed that there is an upward trend in the number of filings every year. In addition, money-service businesses and the securities/futures area had high growth rates, which points to a wider coverage net in various industries. At the same time, the average time of processing increased to 43 days, as opposed to 32; this is an indication of building workloads and systemic pressure. Overall, the trend identified can be taken as a sign of not only improved reporting but also the problems involved in dealing with the increasing load of SARS.

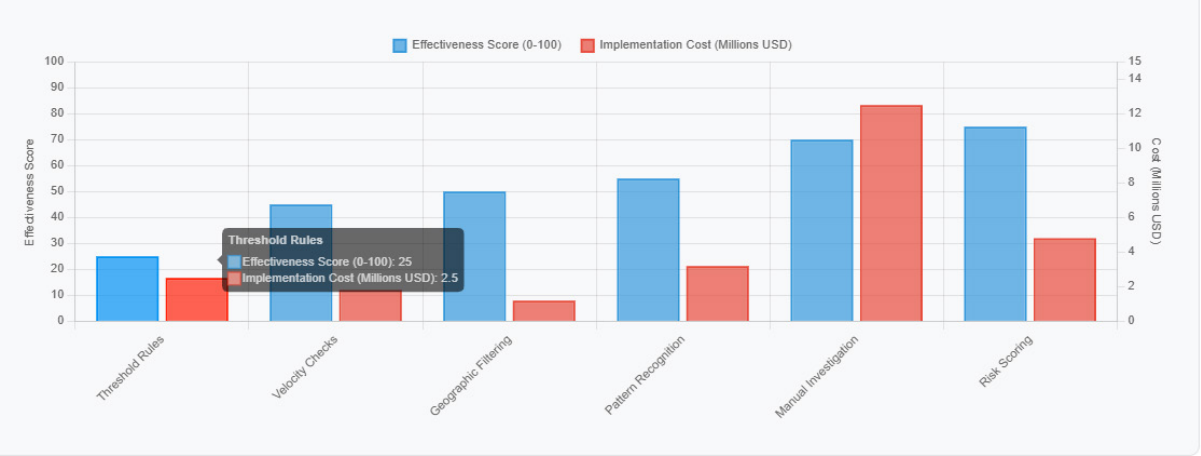

Figure 2: Traditional AML Detection Method Effectiveness vs. Implementation Cost

The chart compares the scores of effectiveness and cost of implementation of the conventional anti-money laundering detection methodology. The threshold rules have a moderate efficacy of 25 and a comparatively low capital outlay. Through comparison, velocity checks and geographic filtering are moderately effective and have a relatively low-cost profile. Pattern recognition algorithms are slightly more effective than they are, but they require a more significant financial investment. The manual investigative procedures are also characterized by a high level of efficacy of 70, though at the highest cost, which is over twelve million dollars, a result that could be explained by the fact that they are labor-intensive. Finally, the risk-scoring methodologies are the most effective with the highest score of 75 and a medium cost level, thus becoming the most fair in terms of the trade-off between the value provided and the cost.

Machine Learning Applications in U.S. Financial Crime Detection

West and Bhattacharya (2016) conducted an extensive review of intelligent financial fraud detection approaches by way of over fifty scientific papers from the period 2004-14 to form a framework for Computational Intelligence-based systems governing fraud detection. They investigated the progression from traditional manual detection to more advanced AI-based detection, which exposes the key shortcomings of rule-based systems with very high false positive rates (95-99%), long processing times and they are not able to learn new fraud patterns. They have evaluated different computational intelligence-based approaches like neural network, support vector machine and ensemble method, which confirms that AI-based platforms have a clear advantage over statistical models in terms of accuracy, flexibility and computation

time. Their hierarchical classification model uncovered voids in the association of fraud types to detection algorithms and performance measures, which lay the basis for future AI-supported fraud detection research. The authors discussed the shift between reactive to proactive fraud detection models and concluded that CI is thinking about financial crime detection in an altogether new way rather than just being a leap forward in computational technology for fraud prevention (Agboola, 2025).

Choi and Lee (2018) have presented a review of artificial intelligence methodologies for financial fraud detection in IoT environments, and they discussed the specialized problems introduced by mobile transactions and device ecosystems. The authors examined the use of deep learning models, specifically Long Short-Term Memory (LSTM) networks, for analyzing sequential transaction records in high-velocity mobile payment scenarios. Empirical validation through the use of Korean financial transaction data from 9/2015 further revealed that their proposed neural architecture provided an accuracy rate of 97.3% as well as a processing speed exceeding 10,000 transactions per second, along with an average response time of less than 50 milliseconds. Authors in another work researched the capabilities of edge computing for IoT fraud detection, so that risk assessment may be done at the device level before transmitting data to centralized processing systems. Distributive architecture with Apache Kafka, Apache Storm and Redis was found to be essential when attempting to keep transactions per second rates at sub-second response times during fraud detection in a high-velocity transaction context.

Njoku *et al.* (2024) carried out a study on machine learning techniques for webpage-based fraud detection systems in Banking, discussed the hybrid system by combining multiple algorithms with the rule-based and to improve the performance and reliability of such a system. Their work evaluated ensemble methodology incorporating Random Forest for pattern recognition, Support Vector Machines (SVM) for boundary detection and gradient boosting for sequential learning in contrast to single models' code-style approaches and achieved better results. Their study covered operational concerns, such as MLOps best practices, automatic model retraining workflows, A/B test frameworks and rolling out new model versions slowly. Their study explored fundamental integration challenges in reproducing AI-driven apps across legacy bank infrastructure, including backward compatibility and adherence to standard security protocols (Gokah *et al.,* 2025). From their review of API-based integrated solutions, the authors discovered that ensuring operational continuity during migration from legacy rule-driven systems to AI-based fraud detection compilers is vital.

Popoola (2024) researched big data-driven financial fraud detection and anomaly detection systems, investigating their impact on regulations compliance and stability of the market in today's financial landscape. Her study evaluated the disruptive nature of analyzing enormous volumes of structured and unstructured data from multiple sources, such as transactional records, consumer behavior and external entity data to discover complex fraud strategies. Her research focused on unsupervised learning techniques, such as clustering algorithms and anomaly detection methods, which were shown to reduce false positive rates by 60-80% relative to rule-based systems while maintaining detection sensitivity above 92%. The author prioritised key implementation challenges such as data privacy, computational overhead and attacks on AI models (adversarial examples) in their research and identified the need for privacy-preserving ML techniques like differential privacy and federated learning as powerful solutions. The inspection revealed that continuous monitoring through automated feature generation employing deep learning approximates a 15-20% increase in accuracy of fraud evasion detection for advanced business scenarios.

Islam and Rahman (2025) explore AI-based fraud detection in financial firms, focusing on holistic approaches for implementing machine learning workflows to address emerging security challenges in the banking industry. Their study compares the claimed benefits of artificial intelligence technologies such as supervised and unsupervised learning algorithms, deep learning architectures, and anomaly detection techniques with traditional rule-based systems, noting the superior performance of the AI methods. Their work also examines key barriers to implementation, including algorithm and data distribution bias, risks related to privacy and regulatory compliance and ethical issues surrounding trust, responsibility and security when deploying AI systems. Their research investigated how AI-based systems can maintain detection rates above 92% even as fraud strategies evolve, using longitudinal performance analyses with ensemble methods to improve robustness against concept drift and adversarial perturbations. Their discussion of explainable AI approaches, such as LIME and SHAP methods, employs understandable machine learning models that are essential for regulatory compliance, customer dispute resolution and audit trail requirements in next-generation financial institutions.

National Security Applications and Inter-Agency Collaboration

Sharing of financial information between the federal government and the private institutions is a key pillar of national security policy. The USA PATRIOT Act, section 314(a), empowers FinCEN to act as an intermediary between the law-enforcement agencies and financial institutions to facilitate the location of accounts and transactions involving suspicious persons or organizations (England, 2023). In the 2023 fiscal year, about 14,000 financial institutions had attended this program, with 588 requests responding to 71 law-enforcement agencies, which concerned 4,606 individuals and yielded over 55,000 responses (Network, 2024). In addition to this, Section 314(b) allows financial institutions to voluntarily

disclose information to each other, as a result forming collaborative networks that find concealed criminal or terrorist financing structures (Network, 2024). These processes demonstrate how laws have changed to strike a balance between the privacy issues and the intelligence requirements of national security investigations.

In addition to the statutory systems that still exist to oversee financial surveillance, in recent years, financial intelligence units (FIUs) and compliance departments have progressively applied more advanced analytical protocols to handle the millions of Suspicious Activity Reports (SARS) that are produced each year (Lagerwaard, 2023). The integration of artificial intelligence and cross-institutional data repositories has significantly enhanced the identification of complex money-laundering and terrorist funds systems that cut across jurisdictions (Redhead, 2021). Through this integrative infrastructure, near real-time intelligence can be shared between FinCEN, law enforcement agencies and private financial institutions, meaning that emergent threats can be identified on a higher level of acuity. Therefore, inter-agency cooperation has become both a significant point of U.S counter-terrorism funding policy, combining legislative power, industry cooperation, and technological innovation to enhance the effectiveness of the prevention of financial crimes.

Table 3: Inter-Agency Financial Crime Collaboration Framework)

Agency/ Department	Primary Role	Key Capabilities	Annual Cases	Budget Allocation (FY2024)	Personnel Assigned	Success Rate
Treasury/ FinCEN	Financial Intelligence Analysis	BSA data analysis, SAR processing, 314(a) coordination	2,300,000	$127.5M	425	92%
Treasury/ OFAC	Sanctions Enforcement	Economic sanctions, asset freezing and designation authority	1,247	$48.3M	175	89%
DOJ/ Criminal Division	Federal Prosecutions	MLAT requests, extraditions and asset forfeiture	3,456	$295.7M	856	87%
FBI/Financial Crimes	Investigations	Undercover operations, HUMINT, cyber investigations	2,178	$445.2M	1,250	84%
DHS/ICE-HSI	Border Security	Trade-based ML, bulk cash smuggling, cryptocurrency	1,834	$234.6M	678	81%
DEA/ Financial Unit	Drug Proceeds	Narcotics financial investigations, asset seizure	4,567	$156.4M	234	88%
IRS-CI	Tax & Financial Crimes	Financial analysis, tax evasion and structuring cases	2,891	$89.7M	312	91%

The cooperation between agencies of the U.S. in the area of financial crime interdiction is outlined in the table provided above and has a clearly defined but complementary scope of operation. FinCEN is at the forefront of the collection and sharing of financial intelligence since more than 2.3 million cases have been processed within the latest fiscal year, with a success rate of about 92 percent. The imposition of sanctions is made by the OFAC and the federal prosecutions are pushed by the Department of Justice; cross-border cooperation is supported as well. The Federal Bureau of Investigation and Department of Homeland Security undertake undercover, cyber and border-related searches for financial misconduct. In the meantime, the Drug Enforcement Administration and the IRS Criminal Investigation Division are strengthening these measures by pursuing drug proceeds and tax-related offences, hence making sure that a national approach is coordinated.

The chart shows that there was a persistent increase in the number of financial crime enforcement actions in the 2019-2024 period. Money laundering cases, in particular, are predominant and increased to about 2024, with around 1,450 cases in 2019. Similarly, the asset seizures have been shown to rise; whereas they were slightly above 2 billion in 2019, they have risen to nearly 3 billion in 2024. The cases of international cooperation also demonstrate a gradual increase, which is also reflected in the number of cases of such cases. The number of terrorist-financing cases, although it remains relatively small, has grown in an incremental, though small, yearly rate. Combined, these tendencies highlight an expansionary course in enforcement, increased recoveries and increased international collaboration in combating financial crime.

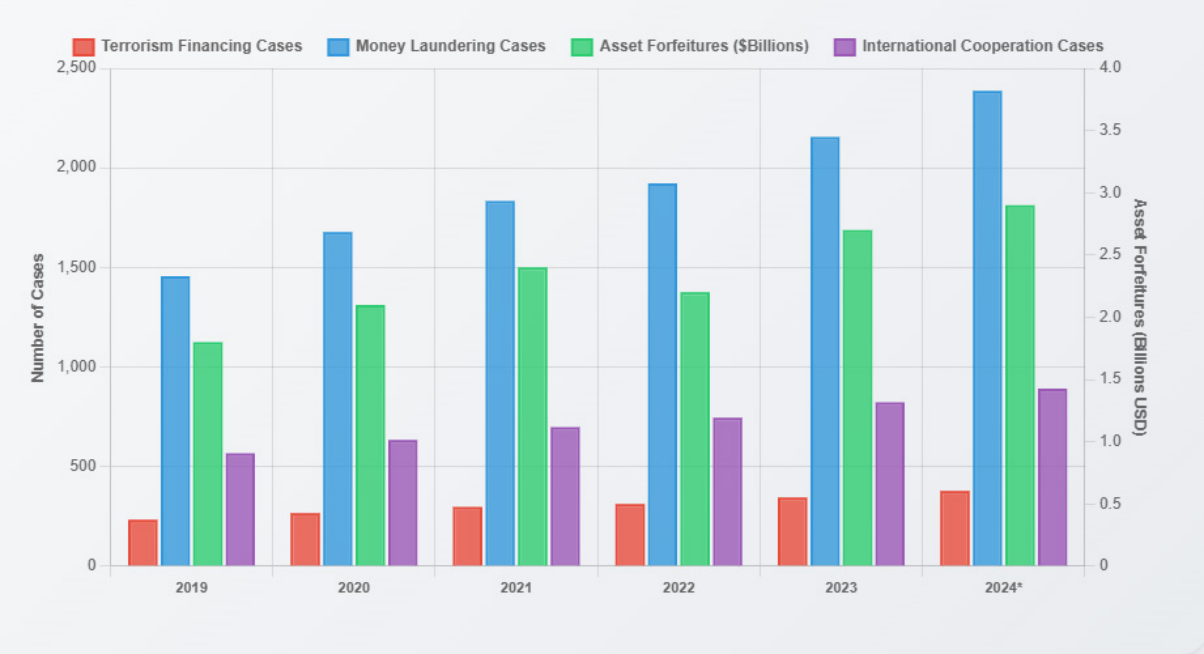

Figure 3: Inter-Agency Financial Crime Investigation Outcomes (2019-2024)

CONCLUSION

Machine learning technologies have the potential to significantly increase the U.S. financial crime detection system and also strengthen national security. Traditional rule-based schemes, however, are heavily limited, with false positives often ranging from 95 to 99%. Furthermore, these approaches lack the capability of evolving with changing criminal patterns and handling the vastness and complexity of modern financial transactions. Machine learning, on the contrary, provides a more resolute substitute, which can adjust permanently and process on a large scale. Current research proves that these machine-learning systems have a detection accuracy of between 92 and 97 percent. They also significantly reduce the false positives by 60 to 80 percent and at present, hardware, as much as ten thousand transactions per second in real time are possible, thus making it suitable in high-frequency financial settings. Bank Secrecy Act, USA PATRIOT Act, and FinCEN regulations are only a few pieces of legislation that have offered a good platform on which these advanced technologies can be deployed. Notably, these laws maintain significant compliance standards and feature inter-agency coordination, which ensures that emerging tools do not contradict the current regulatory requirements. The results of the work on collaborative frameworks further prove the effectiveness of this method. These programmes have been effective in more than 90 percent of the cases through a collective analysis of over 2.3 million cases each year, which further explains why incorporating new technology into traditional institutional partnerships is effective. Finally, machine learning-driven proactive detection as opposed to reactive detection can be seen as a paradigm shift in the United States' financial infrastructure protection. Such evolution increases the protective action and strengthens the democratic institutions against economic warfare and financing the network of terrorists, thus overcoming the essential national security issues in our more connected global economy.

REFERENCES

Adaji, C. C., Bello, A. A., Ukatu, C. E., Okika, N., Agboola, O. K., & Amomo, C. G. (2025). AI-powered cybersecurity governance: The role of business analysts in ethical AI deployment. *International Journal of Innovative Science and Research Technology, 10*(3), 1384–1396. https://doi.org/10.38124//ijisrt/25mar924

Adukpo, T. K., & Bethel, J. O. (2025). Impact of macroeconomic factors on government spending in Ghana. *American Journal of Applied Statistics and Economics, 4*(1). https://doi.org/10.54536/ajase.v4i1.5833

Agboola, O. K. (2025). AI-driven fraud detection and biometric KYC: Enhancing ethical compliance in U.S. digital banking. *International Journal of Computer Applications Technology and Research, 14*(8), 112–121. https://doi.org/10.7753/IJCATR1408.1010

Agboola, O. K. (2025). Auditing bias in AI and machine learning-based credit algorithms: A data science perspective on fairness and ethics in FinTech. *International Journal of Technology Management, 11*(2), Article 10. https://doi.org/10.21590/ijtmh.11.02.10

Agboola, O. K. (2025). The role of behavioural economics in understanding and countering fraudulent tactics. *IOSR Journal of Economics and Finance, 16*(4, Series 1), 8–12. https://doi.org/10.9790/5933-1604010812

Agboola, O. K., & Alabi, K. O. (2025). Predicting systemic financial crises with AI and machine learning: A macroprudential data science approach in the US

context. *International Journal of Research Publication and Reviews, 6*(8), 5121–5136.

Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in the financial domain. *Future Generation Computer Systems, 55*, 278–288. https://doi.org/10.1016/j.future.2015.01.012

Aidoo, S., AML, I. D., AML, M., & Expert, F. C. C. (n.d.). *Transaction monitoring and suspicious activity reporting (SAR).*

Akankpo, U. E. (2025). Economic crimes of terrorism (ECT): *Implications for global growth and development.*

Allegrezza, S. (2022). The proposed anti-money laundering authority, FIU cooperation, powers and exchanges of information: A critical assessment. *University of Luxembourg Law Research Paper,* (2025-04).

Al-Mansoori, S., & Salem, M. B. (2023). The role of artificial intelligence and machine learning in shaping the future of cybersecurity: Trends, applications, and ethical considerations. *International Journal of Social Analytics, 8*(9), 1–16.

Azcárraga, A. A. P., & San Juan, R. (2022). Strengthening the core customs processes through integrated risk management. In *Strengthening customs administration in a changing world* (pp. 131).

Brito, J., & Castillo, A. (2013). *Bitcoin: A primer for policymakers.* Mercatus Center at George Mason University.

Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under an IoT environment: A survey and implementation. *Security and Communication Networks, 2018*(1), 5483472. https://doi.org/10.1155/2018/5483472

Colella, F., Maskus, K. E., & Peri, A. (2025). Unintended consequences of anti-money-laundering regulations. *The Economic Journal, ueaf086*. https://doi.org/10.1093/ej/ueaf086

Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications, 67*, 49-58. https://doi.org/10.1016/j.eswa.2016.09.029

Collin, M., Cook, S., & Soramaki, K. (2016). *The impact of anti-money laundering regulation on payment flows: Evidence from SWIFT data* (Working Paper No. 445). Center for Global Development.

Council, F. F. I. E. (2005). *Bank secrecy act anti-money laundering examination manual.* Federal Financial Institutions Examination Council.

Demetis, D. S. (2010). Technology and anti-money laundering: A systems theory and risk-based approach. In *Technology and anti-money laundering.* Edward Elgar Publishing.

Devaney, J. G. (2025). On sanctions and the enforcement of international law: A rule of law analysis. *Nordic Journal of International Law, 1*(aop), 1-22.

Donohue, L. K. (2008). *The cost of counterterrorism: Power, politics, and liberty.* Cambridge University Press.

England, K. T. (2023). A unified front: The need for a comprehensive, centralized network for financial institutions and law enforcement to collaborate on anti-human trafficking efforts. NC Bank. *Inst., 27*, 284.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal, 6*(2), 2188–2204. https://doi.org/10.1109/JIOT.2018.2882794

Gokah, B. E., Amoako, E. K., Adom, S. G., Abakah, L. K., & Sampson, E. (2025). AI-driven user experience (UX) frameworks to enhance trust and security in U.S. online banking. *Finance & Accounting Research Journal, 7*(9), 465–478. https://doi.org/10.51594/farj.v7i9.2069

Gordon, L., Loeb, M., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model. *Journal of Cybersecurity, 6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Hutchinson, G. (2024). *Money laundering in the United States: A review of current regulations and threats.*

Islam, M. S., & Rahman, N. (2025). AI-driven fraud detections in financial institutions: A comprehensive study. *Journal of Computer Science and Technology Studies, 7*(1), 100-112.

Jennings, A. K. (2025). Criminal investors. *George Washington Law Review, 93*, 851.

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control, 23*(1), 173-186. https://doi.org/10.1108/JMLC-07-2019-0055

Kazeem, T., Agboola, O. K., Okika, N., Owoola-Adebayo, S. F., Opeola, F., Akunna, N. L., & Abimbola, O. S. (2025). Risk management and governance in blockchain-based digital identity projects: A business analysis and project management framework. *ITEGAM–Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA), 11*(54). https://doi.org/10.5935/jetia.v11i54.1710

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12*(10), 417. https://doi.org/10.3390/info12100417

Lagerwaard, P. (2023). Financial surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands. *Journal of Money Laundering Control, 26*(7), 63-84. https://doi.org/10.1108/JMLC-01-2023-0006

Lee, I. (2020). Internet of things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet, 12*(9), 157. https://doi.org/10.3390/fi12090157

Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. *International Research Journal of Modernization in Engineering Technology and Science, 1*(32644). https://doi.org/10.56726/IRJMETS32644

Marklund, A., & Skouvig, L. (2021). *Histories of surveillance from antiquity to the digital era.* Routledge.

Nandy, D., & Al Mamun, A. (2024). Financial crimes through fintech by political leaders: The experience of select South Asian states. In *E-banking, fintech, & financial crimes: The current economic and regulatory landscape* (pp. 79-95). Springer Nature Switzerland.

Narsimha, B., Raghavendran, C., Rajyalakshmi, P., Reddy, G., Bhargavi, M., & Naresh, P. (2022). Cyber defense in the age of artificial intelligence and machine learning for a financial fraud detection application. *International Journal of Electrical and Electronics Research, 10*(2), 87–92. https://doi.org/10.37391/ijeer.100206

Narteh-Kofi, E., Asamoah, E., Adukpo, T. K., Mensah, N. (2025). Mergers and Acquisitions in the U.S. Capital Market: Theoretical Foundations, Market Dynamics and Strategic Implications. EPRA *International Journal of Economics, Business and Management Studies (EBMS), 12*(3), 71-80. https://doi.org/10.36713/epra20500

Narteh-Kofi, E., Raji, Y. M., Asamoah, E., & Adukpo, T. K. (2025). The role of artificial intelligence in enhancing decision-making and efficiency in mergers and acquisitions: A case study approach within the U.S. capital market. *International Journal for Multidisciplinary Research (IJFMR), 7*(3). https://doi.org/10.36948/ijfmr.2025.v07i03.44171

Narteh-Kofi, E., Sampson, E., Hattoh, E., Akingbade, R., & Agbeve, V. (2025, July 30). Optimizing target identification in the U.S. capital market mergers and acquisitions through artificial intelligence: Implications for financial efficiency, compliance, and national economic competitiveness. *International Journal for Multidisciplinary Research (IJFMR), 7*(4). https://doi.org/10.36948/ijfmr.2025.v07i04.51702

Nephew, R. (2017). *The art of sanctions: A view from the field.* Columbia University Press.

Network, F. C. E. (2024). *RE: Notice of proposed rulemaking on anti-money laundering and countering the financing of terrorism programs* (docket number FINCEN–2024–0013). Policy.

Ng, A., & Kwok, B. (2017). Emergence of fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance, 25*(4), 422–434. https://doi.org/10.1108/jfrc-01-2017-0013

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access, 9*, 163965-163986.

Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for a fraud detection system in a financial institution: A web-based application. *Machine Learning, 20*(4), 01-12.

Ogunjide, J., Oluwatobi, Awowole, A. O., Adamaagashi, I., Prince, & Agboola, O. K. (2025). Relationship between biometric technology and customer satisfaction in the fintech sector. *IIARD International Journal of Economics and Business Management, 11*(4), 190–204. https://doi.org/10.56201/ijebm.vol.11.no4.2025.pg190.204

Oyinkansola, A. B. (2024). The gig economy: Challenges for the tax system. *Journal of Knowledge Learning and Science Technology, 3*(3), 1–8.

Panico, P. (2025). *Trusts without equity: A comparative and transnational perspective* [Doctoral dissertation, University of Portsmouth].

Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customers' data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing, 14*(3), 01-16.

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice, 3*(1), 73-94. https://doi.org/10.1080/25741292.2020.1725366

Pomerleau, P. L., & Lowery, D. L. (2020). *Countering cyber threats to financial institutions: A private and public partnership approach to critical infrastructure protection.* Springer.

Popoola, N. T. (2023). Big data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability. *International Journal of Computer Applications & Technology Research, 12*(09), 32-46.

Raghuwanshi, P. (2024). AI-driven identity and financial fraud detection for national security. *Journal of Artificial Intelligence General Science, 7*(01), 38-51.

Redhead, M. (2021). *The future of transaction monitoring: Better ways to detect and disrupt financial crime* (SSRN Working Paper No. 3821545).

Ross, S., & Hannan, M. (2007). Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control, 10*(1), 106-115. https://doi.org/10.1108/13685200710721881

Sampson, E., & Narteh-Kofi, E. (2025). Digital sales transformation in Sub-Saharan Africa: Impacts on cross-border trade and global market integration. *World Journal of Advanced Research and Reviews, 27* (3), 1092–1101. https://doi. org/10.30574/wjarr, 3.

Sani, Z. N., & Aryee, B. A. (2025). Optimizing drug supply chains to prevent shortages in rural U.S. hospitals. *EPRA International Journal of Economics, Business and Management Studies.* https://doi.org/10.36713/epra24022

Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Española de Documentación Científica, 15*(4), 42–66. https://doi.org/10.3989/redc.2021.4

Shihembetsa, E. (2021). *Use of artificial intelligence algorithms to enhance fraud detection in the banking industry* (Doctoral dissertation, University of Nairobi).

Stevens, H. (2022). *Why financial institutions continue to violate anti-money laundering laws and regulations: Exploring the differences between compliance and non-compliance* [Master's thesis, Utica University].

Syafrizal, M., Selamat, S., & Zakaria, N. (2022). Analysis of

cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3). https://doi.org/10.17762/ijcnis.v12i3.4817

Turner, J. E. (2011). *Money laundering prevention: Deterring, detecting, and resolving financial fraud*. Wiley.

Umoh, B. U., Bello, A. A., Okika, N., Ukatu, C. E., & Agboola, O. K. (2025). The intersection of artificial intelligence and human decision-making in cybersecurity resilience: Business analysis perspective. *CogNexus, 1*(2), 26–36. https://doi.org/10.63084/cognexus.v1i02.58

Wen, J., Zhao, X., & Chang, C. P. (2024). The impact of international sanctions on the innovation of target countries. *Economics & Politics, 36*(1), 39-79. https://doi.org/10.1111/ecpo.12239

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47-66. https://doi.org/10.1016/j.cose.2015.11.006

Yakubu, S. (2017). *A critical appraisal of the law and practice relating to money laundering in the USA and UK* [Doctoral dissertation, School of Advanced Study, University of London].