Available on: https://jefrr.ep-journals.org/ E-ISSN: 3051-3650, P-ISSN: 3051-3642

Journal of Economic Finance Research and Review

Volume: 02 Issue: 08 August 2026

Comparing U.S. and Approaches to AI-Driven Fraud Prevention

Afari Ntiakoh
University of Nevada, Reno, USA

Christian Amoakoh
Illinois State University, USA

Deborah Akuele Apaflo
University of Ghana - Legon, Accra, Ghana

Yeboah Mary Magdalene
University of Ghana Business School, Ghana

Published Date: August 03, 2026 **Article DOI: 10.65150/EP-jefrr/V2E8/2026-02**

ABSTRACT: The increasing sophistication of financial and cyber fraud has led national governments, banks and regulators globally to incorporate artificial intelligence (AI) into anti-fraud measures. This paper compares the reactive, decentralized approach adopted by the United States and more prescriptive, risk-based regulatory models embraced by global peers such as the European Union and the United Kingdom. By referencing academic studies, regulatory documents, and case studies of institutions, the paper covers how these tools (like machine learning (ML) models, biometric authentication, and real-time transaction monitoring) are used to detect and prevent fraudulent behavior, including identity theft and new generative-AI-driven scams. It also examines how different regulatory environments influence the adoption of AI and technology, with a focus on the intersection among innovation, compliance, privacy, and ethical governance.

The results indicate that the U.S. model, with its flexibility and quick adaptability by sectors, can result in fractured oversight structures and breaks in compliance and accountability. In contrast, international approaches, including the EU's AI Act and UK proposals, emphasize transparency, standardization, and risk reduction, but may restrict innovation through stringent regulatory demands. Effective AI-enabled fraud prevention demands common international standards, ethical AI governance, and enhanced cross-border data sharing mechanisms. It serves as a hero to transform global financial security and regulatory collaboration in the age of intelligent fraud detection.

KEYWORDS: Fraud prevention, Artificial Intelligence, Data Privacy, Machine Learning, Regulatory Compliance.

INTRODUCTION

The pace of digital commerce and financial technology's development has been disappointingly matched by the growth in complexity and magnitude of fraud, making it a universal problem throughout the world (Ntiakoh et al, 2026). Traditional rule-based detection systems have become increasingly futile against the most recent (some AI-enabled) fraudulent tactics, resulting in significant financial losses for consumers, businesses, and nations in general (Singh, 2025). To address this pressing problem, revolutionary technology enabling future fraud solutions is Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL). These AI-based solutions screen enormous and various transaction databases at scale in real time, utilizing predictive analytics and novel behavioral biometrics to recognize complex patterns (Popoola, 2023) as well as subtle anomalies that escape traditional tools. This is reflected in the fact that the worldwide market for AI in fraud detection and prevention continues to grow fast, reflecting its indispensability with respect to securing today's financial and digital ecosystem. This article offers a comprehensive and in-depth academic insight into the subject by contrasting the innovative technological, regulatory regimes of the US respectively and the rest of global jurisdictions, particularly that of EU region, with reference to AI-powered fraud prevention.

The US model of AI and financial fraud prevention combines rapid technological development, heavy reliance on private sector investment in innovation, and an expanding, fragmented regulatory (sector targeting) architecture (Agbadamasi et al., 2025). The U.S. is the largest market for global fraud detection technology, with a large concentration of leading AI service providers and high volumes of digital transactions, which constantly provide good and refine advanced ML regulations. The Gramm-Leach-Bliley Act (GLBA) and the Bank Secrecy Act (BSA) have been forcing financial institutions toward bleeding-edge AI for automated compliance checks, AI/ML monitoring, and real-time fraud detection, although not in a direct manner.

In sharp contrast, many countries worldwide, including at least the European Union, consider that thorough and rights-based precautionary regulation should be the rule rather than focusing on quick sectoral rollout. The first pillar of the EU's ethical approach to data is founded in legislation (such as GDPR). It requires robust technical and organizational measures to be implemented, with an emphasis on minimizing data use and purpose limitation (Osifowokan et al., 2025), together with a broad conceptualization of individual control and privacy rights that has

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

established high-level global standards for what constitutes ethical approaches to using personal data (Agbadamasi et al., 2025). This is underpinned by the prospective AI that categorizes AI systems, including credit score or fraud detection systems, by their risk (Hasan, M. et al., 2025). Such high-risk systems would be exposed to strict transparency obligations, auditability, and human oversight, as well as requirements to prevent biases (Valsa Saratchandran, 2025), with direct implications for how their AI fraud solutions are currently designed and deployed by EU financial institutions.

LITERATURE REVIEW

Advanced Machine Learning Methods and Improved Efficiency

Modern research has demonstrated very good results of custom ML algorithms for processing enormous, high-velocity streams of data to detect complex non-linear patterns of fraud. AI-based approaches, employing Deep Learning principles such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks for sequence recognition, can reach detection rates, cutting false positives against traditional tools. On the other hand, graph neural networks (GNNs) have been a strong alternative for modeling relational data manifested in financial transactions by effectively detecting coordinated fraud and money laundering activities (Kaja, 2023) with high accuracy through the analysis of network relationships between accounts and transactions. The underlying technology capability rests on real-time anomaly detection using the behavioral biometric that learns about and flags slight, suspicious deviations from the user's known transactional and digital behavior (Rajapaksha, 2022).

Hybrid Frameworks and Innovation Gaps

To manage the trade-offs between performance and trustworthiness, hybrid frameworks are widely applied in industry, which combine the predictive accuracy of ML with the governance advantages of rule-based logic. Moreover, the integrated systems themselves are AI-based and can improve their detections based on new alerts, increasing both efficacy and interpretability (Alketbi, K.S. et al., 2025). Nonetheless, the literature also notes a general 'blind spot' since there is not enough reportage on online learning techniques, which could lead to real-time response in some way; academic research seems to lag actual practice.

The U.S. Market-Driven Sector-Specific Regulation

The U.S. regulatory policy is largely market-based and disaggregated, which emphasizes industry-oriented, rather than holistic federal AI law. Such a perspective is mainly oriented toward economic progress and technological domination. Compliance needs to fulfill the regulation requirement according to the Bank Secrecy Act (BSA) and Gramm-Leach-Bliley Act (GLBA) (FFIEC, 2014), which can be satisfied by adopting technological solutions such as advanced analytics with respect to AML or KYC, enabling U.S. financial institutions to use technology and achieve operational agility (Nwangele, C.R. et al., 2023). However, this system presents a major pitfall: the lack of a nationally ratified data protection standard means sifting through a patchwork of state-based laws, such as the California Consumer Privacy Act (CCPA), that complicates data aggregation, which is necessary for training precise and generalizable AI models while often hindering consistent enforcement and unified federal oversight.

The EU Precautionary, Rights-Based Governance

By contrast, the European Union insists on a precautionary and rights-based approach, through comprehensive regulation which establishes "a global gold standard for ethical oversight of AI". It is based on the principle that allows the minimization of data, penalized by the GDPR (General Data Protection Regulation), and from which people can claim for solely automated decision making (Brkan, 2019). This has direct implications on the use of Explainable AI (XAI) techniques to make sure that fraud decisions made by AI are auditable, interpretable, and conform with transparency requirements (Olawore, S.O. et al., 2025). The new EU AI Act also reflects this trend by differentiating between risk categories and thus bringing AI systems for fraud detection as a "high-risk" application under a stricter microscope with higher expectations in data quality, bias testing, and human control. Although less flexible to the pace of innovation and more costly for the industry, this straitened regulatory framework is best known for its advanced capability in supporting ethics-centered preemptive measures against algorithmic biases and abuses, ensuring that implementation of technologies is guided by fundamental human rights regulations and public accountability.

Mutual, Ethical, and Organizational Implementation Challenges

Algorithmic Bias, Fairness, and Accountability

A common problem in all these jurisdictions is the widespread risk of algorithmic bias, as AI models can encode and propagate societal discrimination present in training data causing them to produce discriminatory fraud flagging against certain demographic groups (Montasari, 2024). Literature recommends the use of specialized methods, such as adversarial debiasing and challenging for 'fairness' during model development to mitigate against bias (Amoako et al., 2025). In addition to this practical concern, the need for XAI, as impelled by European Union (EU) regulations, is also common to both because "black box" deep learning models prevent accountability and human control, which creates a liability crisis when it comes to automated decision making. Achieving algorithmic fairness is paramount, with research exploring methods like adversarial debiasing and the imposition of fairness constraints during model training to ensure equitable outcomes. The issue of liability is also slated for increased focus, especially in the EU, through proposed AI Liability Directives, which may impose stricter disclosure responsibility and defect liability in AI systems.

Data Quality, Privacy, and Adversarial Threats

The efficiency of AI models depends essentially on high-quality data as well as timely availability. This need is in stark contrast with various international data protection regimes, not least the General Data Protection Regulation (GDPR), which demands minimization of processing and limitation as to purposes (Marelli, L. et al., 2024). This complexity is further complicated with the introduction of AI-based fraud-breaching systems by creating deep fakes and synthetic identity activities that force financial institutions to integrate complex defenses (adversarial machine learning and multi-modal data analytics) even for their detection systems themselves (Amoako et al., 2025). These threats cross borders rapidly, but the capacity to respond differs. U.S. institutions are often quicker to adopt cutting-edge detection tools, whereas in global settings, deployment lags due to limited data, fewer skilled practitioners, and stricter legal barriers for data sharing.

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

Organizational Constraints and Scalability

Organizational barriers, including resource limitations, lack of technology experience, and scalability, are the major reasons hindering the widespread application of AI (Omokhoa H.E. et al., 2024). Although AI is highly scalable, the high investment cost and complexity of implementation of advanced models are major challenges, particularly for smaller financial institutions (Kadioglu, Y.M. et al., 2024). These institutional and infrastructural constraints result in unequal enforcement capacity, with US institutions and global partners having differing enforcement capacity across states or regions. These leave less technologically mature regions and small institutions vulnerable, thereby creating weak exploitable links in the international anti-fraud defense network. This problem is rooted in profound resource gaps and high investment barriers, as the substantial capital required for high-performance computing, quality data infrastructure, and the recruitment of scarce, expensive AI and data science talent is often prohibitive.

FINDINGS AND DISCUSSION

This chapter reports and discusses the results obtained from this study, using the studied literature to reflect relevant trends, technological innovations, and regulatory disparities in relation to AI applied for fraud detection. The analysis is framed around two main sections: the results, focusing on empirical insights and emergent patterns, and a discussion of where these findings fit within wider scholarly and practical conversations. Taken together, these sections should leave the reader with a robust sense of AI-driven fraud prevention systems as both an opportunity and a challenge in the US and EU.

Findings

The empirical results distilled from the literature point toward three clear trends on how AI is being adopted and regulated for financial fraud detection: the technological prevalence of Machine Learning (ML) systems; the stark difference between regulatory philosophies across leading international blocs, including China, the US, and the EU; and shared operational and ethical challenges as a global phenomenon.

Technological Advantage and Predictive Accuracy of AI Mechanisms

The most solid outcome is about the technological superiority of AI and ML compared to traditional rule-based systems, considering contemporary adaptive financial fraud. This superiority is measurable and comes from the use of advanced algorithmic techniques. AI applications with Graph Neural Networks (GNNs) and Deep Neural Networks (DNNs) consistently attain fraud detection rates of 87% - 94% range (Vallarino, 2025), showing the ability to lower the expensive number of false positives by as much as 60% relative to fixed threshold models. In addition, GNNs are also particularly effective when it comes to systemic fraud detection by generalizing across individual transactions and learning complex (Nguyen, L. et al., 2025) non-evident relationships throughout the full financial networks and detecting organized crimes or money laundering schemes that rule-based systems overlook. This predictability proves the breakthrough nature and not incremental innovation of AI technology, essentially because of enabling real-time anomaly detection embedded in behavior biometrics.

Contrasting Regulatory Models and the Trade-Off Between Innovation and Rights

A second finding is the crystallization of two opposed models of regulation: the U.S. market-led, sectoral model and the EU's precautionary, rights-based model. U.S. policy is characterized by piecemeal, non-systematized guidance that relies on the Bank Secrecy Act (BSA), Gramm-Leach-Bliley Act (GLBA), among other laws, to indirectly promote the adoption of AI, prioritizing innovation velocity and market efficiency. Such has been the case with the rapid adoption of state-of-the-art models, which in turn places institutions at risk of managing inconsistent state privacy laws like the California Consumer Privacy Act (CCPA) that fragment data required for effective AI training and present regulatory uncertainty around accountability (Dubey, S. et al., 2024). By contrast, in the EU unified framework, fraud detection is defined as a "high-risk" application through the General Data Protection Regulation (GDPR) and the proposed AI Act (Arda, 2024). It thus proactively places strict requirements on data minimization, bias testing, and human oversight, which are made enforceable by the right of an individual to explanation for automated decisions (Hickman, E. et al., 2021). This model, which will be costly (but potentially less than the cost of bias mitigation on legal exposure and basic data rights) to compliance but whose rate of adoption may lag, if only for pragmatic reasons, is one that has been deliberately constructed to minimize legal risk around bias and to prioritize fundamental data protection rights.

Widespread Ethical and Organizational Asymmetry

This work points to continued shared ethical and organizational challenges that cut across jurisdictions' regulatory borders, preventing the fair and trusted enablement of AI worldwide (Tom Coyne, 2024). Certainly, algorithmic bias is a significant and widespread ethical problem we continue to see. Evidence shows that biased data training results in discriminatory outputs, over-focusing on and flagging transactions of profiles owned by demographic groups (Aarvik, 2019). More operationally, the same sector must deal with adversarial threats as fundamental to doing business, where generative AI has been weaponized for synthetic identity fraud, fake documents, and deepfakes, there is simply no option other than relentless investment in counters. Fundamentally, constraints of the organization and asymmetries in resources are noted by a huge investment floor and deep technical expertise shortfalls help to reproduce a structural gap that only allows AI's scale promise to unfold in favor of (very) large financial organizations. Because of those differences, there is an uneven capability for enforcement by the smaller institutions and regional agencies, which global fraudsters are quick to exploit.

DISCUSSION

The debate revolves around the fundamental trade-off between AI's increased predictability performance and the need for model explainability (XAI), which forms a trust crisis in automated decision-making. Deep learning models produce the best performance however, they are inherently opaque "black box" systems and run against regulation demands for transparency (de Carvalho Souza et al., 2025), such as that of EU's right to explanation. This tension is not just technological, but also legal and ethical decisions that result in freezing accounts or cutting off financial services must be accountable to those affected and auditable by regulators. Researchers advocate that to persist in the use of precision, low transparence models risk undermining public trust and raising legal risk (Oluwafemi, I.O. et al., 2021). Hence, a change of course is needed where Explainable AI (XAI) frameworks, such as those that leverage methods like SHAP (Shapley Additive exPlanations) or LIME (Local Interpretable

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

Model-agnostic Explanations) are preferred to make transparency an integral part of the model development process from the beginning instead of just an annexed requirement.

Policy Relevance of Regulatory Divergence and Future Harmonization

The differing regulatory trajectories in the U.S. and EU illustrate a critical policy choice at stake with global implications to foster and enable innovation or pursue ethical rigor and protection of fundamental rights. U.S. model decentralized evolution of enforcement for anti-bias and privacy regulations, with inherent regulatory lag, with consumers open to potential lurking systemic algorithmic bias that a unified federal mandate could partially address pre-emptively. In contrast, the EU's policy of the precautionary principle enhances trust through requirements for XAI and bias testing, but its concrete costs must also be considered. They may inadvertently hamper the swift deployment of technology and impose on European firms. A possible way forward will be harmonization of the policies across the globe, which may also include a hybrid model, where US' agile market-driven development can still exist, but impose high-risk applications such as fraud detection to comply with mandatory pre-market conformity assessment and rigorous accountability requirements.

The Case for Collective Resilience and Public-Private Action

The argumentation on systemic vulnerabilities must come to the realization that the prevalence of organizational constraints and asymmetrical resources is a market failure, not simply an operational issue. It is the collateral effect of smaller FIs and regional enforcers not being able to invest in AI talents and infrastructure that traditional financial system integrity itself will be compromised (Aidoo, 2025). Responding to this will require major shifts away from the market-based private sector solutions toward resilience mechanisms for collective action. This would involve promoting the public-private partnership to finance government-backed AI resource sharing and federation learning models' deployment (Khan, H.H. et al., 2020). These would enable smaller actors to train accurate, de-biased AI on pooled but encrypted data without legal infringements, democratizing state-of-the-art defense against fraud and even leveling the playing field that favors transactional criminal networks.

CONCLUSION

This study demonstrates the revolutionary power of AI in changing the way we do things around here, from preventing financial and cyber fraud to helping redefine battlefield support methods on a global scale. In this comparison between U.S. and international perspectives, AI systems powered by machine learning, behavioral analytics, and real-time monitoring are key to achieving greater detection accuracy and operational efficiency. America's model showcases innovation and emphasizes the flexibility of AI deployment with existing compliance programs, such as Know Your Customer (KYC) and Anti-Money Laundering (AML). Conversely, several international jurisdictions, including the European Union and United Kingdom, have favored structured risk-based regulatory regimes with an emphasis on transparency, accountability and ethical governance. Notwithstanding such diversity in their methods, these models share common challenges of algorithmic bias, data privacy issues and cybersecurity-threat exposures that advocate for the development of AI systems to be an ongoing process.

Ultimately, the study finds that the future of AI for fraud prevention will be in international cooperation that balances innovation with accountability. The establishment of unified international standards, encouragement for ethical AI governance and improvement of cross-border data-sharing mechanisms can exhibit their maximal efficiency. Incorporating these idealized principles, regulators and the financial industry can construct vigorous, transparent, and malleable frameworks that are ready to respond to increasingly complex financial fraud. Over the long run, AI's ongoing influence will rest on finding the appropriate balance between regulatory stringency and technological flexibility in a way that ensures the integrity of global financial networks.

REFERENCES

1) Aarvik, P. (2019). Artificial Intelligence–a promising anti-corruption tool in development settings. *U4 Anti-Corruption Resource Centre*.
2) Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., & Mensah, N. (2025). Navigating the intersection of US regulatory frameworks and artificial intelligence: Strategies for ethical compliance. World Journal of Advanced Research and Reviews, 25(3), 969-979.
3) Aidoo, S., & AML, I. D. (2025). Regulatory Frameworks for Combating Financial Crime in Emerging Markets.
4) Ali, F. (2024). PRIVACY BY DESIGN: STRENGTHENING DATA PROTECTION IN DIGITAL COMMUNICATION. *International Journal of Information and Communication Technology Trends*, *4*(1), 116-124.
5) Alketbi, K. S., & Mehmood, A. (2025). A Comprehensive Survey of Explainable Artificial Intelligence Techniques for Malicious Insider Threat Detection. *IEEE Access*.
6) Amoako, E. K., Okeke, P. T., Boateng, V., Bonsu, M. A., & Oman-Amoako, M. (2025). Enhancing risk management and fraud detection in the U.S. financial industry through machine learning algorithms: Applications, challenges, and future directions. *World Journal of Advanced Research and Reviews, 28*(3), 134–144.
7) Arda, S. (2024). Taxonomy to regulation: A (geo) political taxonomy for ai risks and regulatory measures in the eu ai act. *arXiv preprint arXiv:2404.11476*.
8) Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International journal of law and information technology*, *27*(2), 91-121.
9) Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: global concerns and local responses. *New media & society*, *11*(3), 395-416.
10) de Carvalho Souza, M. E., Souza, M. E. D. C., & Weigang, L. (2025). Unveiling the Black Box: The Significance of XAI in Making LLMs Transparent. *Authorea Preprints*.
11) Dubey, S., & Sharma, R. (2024). The Privacy Paradox: The Future of Personal Data Protection in the Big Data Age. *Issue 6 Int'l JL Mgmt. & Human.*, *7*, 1647.
12) FFIEC, E. C. (2014). Federal Financial Institutions Examination Council. *Bank Secrecy Act/Anti-Money Laundering Examination Manual*.

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

13) Hasan, M., & Faruq, M. O. (2025). AI-Augmented Risk Detection in Cybersecurity Compliance: A GRC-Based Evaluation in Healthcare and Financial Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 313-342.
14) Hickman, E., & Petrin, M. (2021). Trustworthy AI and corporate governance: the EU's ethics guidelines for trustworthy artificial intelligence from a company law perspective. *European Business Organization Law Review*, *22*(4), 593-625.
15) Kadioglu, Y. M., & Soydan, H. (2024). The Transformative Role of Artificial Intelligence in Finance and Economics. In *Artificial Intelligence* (pp. 193-207). CRC Press.
16) Kaja, A. (2023). Self-supervised learning with graphical context to effectively capture complex money laundering activities.
17) Khan, H. H., Malik, M. N., Zafar, R., Goni, F. A., Chofreh, A. G., Klemeš, J. J., & Alotaibi, Y. (2020). Challenges for sustainable smart city development: A conceptual framework. *Sustainable Development*, *28*(5), 1507-1518.
18) Marelli, L., Lievevrouw, E., & Van Hoyweghen, I. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy studies*, *41*(5), 447-467.
19) Mohanarajesh, K. (2024). Develop New Techniques for Ensuring Fairness in Artificial Intelligence and ML Models to Promote Ethical and Unbiased Decision-Making.
20) Montasari, R. (2024). Analysing ethical, legal, technical and operational challenges of the application of machine learning in countering cyber terrorism. In *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses* (pp. 159-197). Cham: Springer International Publishing.
21) Nguyen, L., Boersma, M., & Acar, E. (2025, July). Detecting Fraud in Financial Networks: A Semi-Supervised GNN Approach with Granger-Causal Explanations. In *World Conference on Explainable Artificial Intelligence* (pp. 330-353). Cham: Springer Nature Switzerland.
22) Nwangele, C. R., Adewuyi, A., Oladuji, T. J., & Ajuwon, A. (2023). International Journal of Social Science Exceptional Research.
23) OLAWORE, S. O., OKOLI, C., ABIMBOLA, O., SERIFAT, B. U. U. U. D., OFURUM, A., & LEO, O. (2025). AI-Driven Cybersecurity Governance in Financial Services: Enhancing Ethical Auditing, Automated Compliance Monitoring and Explainable AI for Stakeholder Trust.
24) Osifowokan, A. S., Agbadamasi, T. O., Adukpo, T. K., & Mensah, N. (2025). Regulatory and legal challenges of artificial intelligence in the US healthcare system: Liability, compliance, and patient safety. *World Journal of Advanced Research and Reviews*, *25*(3), 949-955.
25) Oluwafemi, I. O., Clement, T., Adanigbo, O. S., Gbenle, T. P., & Adekunle, B. I. (2021). A review of ethical considerations in AI-driven marketing analytics: Privacy, transparency, and consumer trust. *International Journal Of Multidisciplinary Research and Growth Evaluation*, *2*(2), 428-435.
26) Omokhoa, H. E., Odionu, C. S., Azubuike, C. H. I. M. A., & Sule, A. K. (2024). Leveraging AI and technology to optimize financial management and operations in microfinance institutions and SMEs. *IRE Journals*, *8*(6), 676.
27) Popoola, N. T. (2023). Big data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability. *Int. J. Comput. Appl. Technol. Res*, *12*(09), 32-46.
28) Rajapaksha, C. I. (2022). Machine Learning-Driven Anomaly Detection Models for Cloud-Hosted E-Payment Infrastructures. *Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks*, *6*(12), 1-11.
29) Singh, H. (2025). Evaluating AI-Enabled Fraud Detection Systems for Protecting Businesses from Financial Losses and Scams. *Available at SSRN 5267872*.
30) Tom Coyne, B. A. (2024). Ensuring Ethical AI.
31) Vallarino, D. (2025). AI-Powered Fraud Detection in Financial Services: GNN, Compliance Challenges, and Risk Mitigation. *Compliance Challenges, and Risk Mitigation (March 07, 2025)*.
32) Valsala Saratchandran, D. (2025). Addressing Compliance, Bias, and Transparency in AI Systems. In *The Impact of Artificial Intelligence on Finance: Transforming Financial Technologies* (pp. 299-321). Cham: Springer Nature Switzerland.
33) Afari Ntiakoh, A., Agyeiwaah, A., Amoakoh, C., & Yeboah, M. M. (2026, April). The economic cost of fraud in the U.S. and how AI can reduce these losses. EPRA International Journal of Economics, Business and Management Studies (EBMS), 13(4). https://doi.org/10.36713/epra27019

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