*Sanjeev P. Sahni, PhD**

DOI: 10.51204/Zbornik_UMKP_25133A
Originalni naučni rad

A SCIENTIFIC APPROACH TO COMBATING GLOBAL FINANCIAL FRAUDS: LEGAL, REGULATORY AND TECHNOLOGICAL DIMENSIONS

Abstract: Financial fraud remains a significant global concern that has surpassed borders, weakened financial systems, and contributed to economic instability. This study looks through a scientific lens to analyze financial frauds, making sure to highlight the complexity of their mechanisms and the ever-changing barrier posed to international law and regulatory frameworks. The review paper attempts to categorize fraud into traditional financial crimes, such as securities fraud, tax evasion, and insider trading, and emerging threats from cyber fraud, digital currencies, and decentralized financial systems.

We also aim to determine the efficacy of international legal instruments, such as the Financial Action Task Force (FATF) recommendations, the United Nations Convention Against Corruption (UNCAC), and regional treaties, in detecting, preventing, and prosecuting financial fraud. Furthermore, the study evaluates the use of advanced technological tools, including machine learning, data analytics, and blockchain forensics, in the detection and prevention of financial fraud. With the help of quantitative case studies and empirical data, the presentation provides insights into the effectiveness of present legal and suggests new, scientifically-grounded methodologies for improving the global fight against financial fraud. The conclusion emphasizes the need for an adaptive, holistic framework that combines legal, scientific, and technological resources to combat financial fraud more effectively in an increasingly complex global economy.

Keywords: financial fraud, transnational crimes, international regulation, blockchain forensics, decentralized finance (DeFi).

* Professor of Eminence, Founder and CEO, Sumona Institute of Behavioral Sciences, New Delhi, India, drspsahni@gmail.com.

1. INTRODUCTION

In today's digital and interconnected world, financial fraud has become a multiplex, developing risk that oversteps borders and destabilizes economies. While traditional crimes like securities fraud and tax evasion are still prevalent, newer schemes: such as cyber fraud, crypto scams, and decentralized finance (DeFi) manipulations, are rising fast. As technology continues to expand and reshape global finance, it brings both innovation and new vulnerabilities on the table. Anonymity, legal loopholes, and advanced digital tools are the weak points and tactics which the criminals are utilizing.[1]

Despite the existence of international treaties like the United Nations Convention against Corruption (UNCAC) and guidelines from the Financial Action Task Force (FATF), enforcement is often inconsistent. Gaps in national laws, political reluctance, and the complex nature of cross-border investigations make global cooperation difficult.[2]

This review looks at financial fraud through an objective lens, integrating legal, regulatory, and tech-focused insights. It traces traditional and emerging fraud types, examines how criminals exploit systems, and determines the underpinnings of present international bills. Finally, it highlights the role of technologies like AI, blockchain, and data analytics in detecting and preventing fraud, advocating for a more integrated and adaptive global strategy.

2. LITERATURE REVIEW

2.1. Conceptualizing Financial Fraud in a Global Context

Financial fraud is no longer confined to isolated, traditional crimes; rather, it has become an expansive, transnational threat. The literature consistently classifies financial fraud into two overarching categories: conventional crimes such as tax evasion, embezzlement, and securities fraud, and digitally enabled crimes including identity theft, cryptocurrency scams, and exploitations within decentralized finance (DeFi) systems.[3] The increasing digitization and globalization of financial systems have intensified both the complexity and reach of fraud, with perpetrators often exploiting weak governance and legal loopholes across borders.

Gottschalk argues that fraud should not merely be seen as criminal misconduct but as a systemic outcome of governance failures, weak compliance cultures,

1 M. Button *et al.*, "Fraud and its Relationship to Technological Advancement", *Journal of Financial Crime*, 1/2022.

2 M. Levi, P. Reuter, "Money Laundering", *Crime and Justice*, 34/2006.

3 D. A. Zetzsche, R. P. Buckley, D. W. Arner, J. N. Barberis, "Decentralized finance (DeFi)", *Journal of Financial Regulation,* 2/2020; B. Unger, J. Ferwerda, *Money laundering in the real estate sector: Suspicious properties,* Edward Elgar Publishing, 2011.

and institutional opacity.[4] Button et al. reinforce this view by situating fraud at the intersection of technological advancement and regulatory inertia.[5] These conceptual foundations highlight that financial fraud is as much a symptom of structural deficiency as it is an individual act of deception.

2.2. International Legal Instruments and Enforcement Challenges

The Recommendations of **United Nations Convention against Corruption (UNCAC)** and the **Financial Action Task Force (FATF)** are widely cited for promoting transparency, encouraging mutual legal assistance, and standardizing anti-money laundering (AML) practices. These tools have initiated the development of national anti-fraud laws and increased global awareness around financial misconduct.

Nonetheless, critical barriers remain at the forefront. It has been noticed that the of international fraud laws are fragmented, especially due to inconsistent legal definitions and enforcement disparities. Levi and Reuter emphasize the practical difficulty of cross-border enforcement, noting how political and procedural barriers often undermine international cooperation.[6] These observations suggest that while global legal instruments provide a useful starting point, they are insufficient in isolation.

2.3. Regulatory Frameworks: Strengths and Deficiencies

On the regulatory front, various national and supranational models have been implemented to strengthen corporate accountability and recognise illegal activity. Notable among them are the **European Union's Market Abuse Regulation (MAR)** and the **United States' Sarbanes-Oxley Act (SOX)**, both of which aim to improve transparency and protect whistleblowers. Yet scholars have noted limitations. Sharman argues that the presence of "secrecy havens" and regulatory capture affects effective enforcement.[7] Ferwerda et al. also highlight an over-dependence on financial institutions—especially banks—to serve as the first line of defense against fraud, often without much oversight or incentive features.[8]

---

4 P. Gottschalk, *Policing financial crime: Intelligence strategy, implementation and organizational change,* CRC Press, 2010.

5 M. Button *et al., op. cit*.

6 M. Levi, P. Reuter, *op. cit*.

7 Sharman J. C., *The money laundry: Regulating criminal finance in the global economy,* Cornell University Press, 2011.

8 J. Ferwerda, I. Deleanu, B. Unger, "Strategies to avoid blacklisting: The case of statistics on money laundering", *European Journal on Criminal Policy and Research,* 4/2020.

As new financial advancements take place, old regulatory schemes struggle to remain relevant. Arner, Barberis, and Buckley highlight how FinTech, cryptocurrencies, and DeFi have formed platforms and instruments that often fall external to the existing legal frameworks.[9]

2.4. Technological Tools in Fraud Detection and Prevention

The role of technology in both enabling and combating fraud is a recurring theme in recent academia. New advancements like Machine learning (ML), artificial intelligence (AI), and blockchain forensics have shown quite a lot of potential in finding anomalies, predicting fraudulent behavior, and tracing illicit transactions. Ruan, Wu, and Zhang note that unsupervised ML models—particularly clustering algorithms and neural networks—are especially effective at finding upcoming fraud patterns.[10] Kirkos also aids the leveraging of decision support systems (DSS) in improving fraud risk assessments in enterprise environments.[11]

Blockchain analytics, as described by Weber et al., give tools for locating crypto-asset transactions across decentralized networks, aiding in asset recovery and compliance monitoring.[12] However, these technologies are not without their barriers. Wischmeyer critiques the transparency of AI models, giving a warning that their "black box" nature may pose an issue for legal admissibility and due process.[13] Additionally, Gillis and Shachar explore how privacy laws such as the GDPR can conflict with data-intensive fraud detection methods, particularly when deployed across borders.[14] Nguyen et al. further find practical barriers—including cost, technical literacy, and legal uncertainty—that restricts the widespread adoption of AI-based tools in developing and even some developed jurisdictions.[15]

9 D. W. Arner, J. Barberis, R. P. Buckley, "The evolution of fintech: A new post-crisis paradigm?", *Georgetown Journal of International Law,* 47/2016.

10 Y. Ruan, J. Wu, Y. Zhang, "Using machine learning for financial fraud detection: A systematic literature review", *Expert Systems with Applications,* 212/2023.

11 E. Kirkos, "Assessing corporate fraud risk with decision support systems: A review", *European Journal of Operational Research,* 1/2015.

12 R. H. Weber, D. Staiger, A. Schwarz, "Blockchain-based tracing: Applying blockchain technology for tracking and tracing products in supply chains", *Journal of Law, Information and Science,* 2/2019.

13 T. Wischmeyer, "Artificial intelligence and transparency: A blueprint for improving the regulation of AI", *German Law Journal,* 2/2020.

14 T. Gillis, C. Shachar, "Artificial intelligence and the GDPR: Navigating the regulatory and ethical minefields", *Computer Law & Security Review,* 44/2022.

15 T. T. Nguyen, Q. U. Nguyen, T. H. Nguyen, "Barriers to adopting artificial intelligence in financial fraud detection: A cross-national study", *Information Systems Frontiers*, 24/2022.

2.5. Toward a Multidisciplinary Anti-Fraud Framework

Given the layered and transnational nature of financial fraud, the literature advocates for an integrated approach. Bantekas puts emphasis on the need for alignment between legal, regulatory, and technological dimensions in combating financial crime.[16] This perspective is voiced by institutions such as the **World Bank (2020)** and the **Basel Committee on Banking Supervision (2021)**, both of which put the importance of intergovernmental cooperation, digital infrastructure development, and institutional capacity building.

Such a framework should be well established, adaptive, capable of evolving with emerging financial threats, and anchored in both technical competence and legal accountability. This includes harmonized legislation, coordinated oversight bodies, shared data protocols, and ethical governance of digital tools. No single mechanism can address the challenges posed by global financial fraud. It is only through systemic reform and interdisciplinary collaboration that sustainable, equitable solutions can be achieved.

3. SYSTEMATIC LITERATURE REVIEW TABLE

Author(s)	Year	Focus Area	Jurisdiction	Key Contribution	Relevance to Review
Levi & Reuter	2006	Money laundering	Global	Highlights legal loopholes and cross-border challenges in financial crime enforcement.	Foundational text on global enforcement and limitations.
UNODC	2004	UNCAC implementation	UN States	Details requirements for criminalizing fraud, cross-border cooperation, and asset recovery.	Legal backbone for anti-fraud efforts internationally.
FATF	2023	AML/CFT standards	Global	Sets international standards for anti-money laundering and financial crime regulation.	Core policy benchmark for global compliance.
Button et al.	2022	Tech & structural fraud	UK	Discusses fraud evolution alongside technological development; criticizes reactive regulation.	Supports the argument that fraud is systemic and tech-driven.
Pieth	2016	Legal harmonization issues	Europe / Global	Critiques the fragmented nature of international fraud laws and inconsistent definitions.	Highlights enforcement disparities and legal inefficiencies.
Arner et al.	2017	Fintech & RegTech	Asia & Global	Reviews challenges regulators face keeping pace with fintech and digital assets.	Frames DeFi and cryptocurrency as regulatory blind spots.

16 Bantekas I., "A unified approach to transnational criminal enforcement: Beyond mutual legal assistance" *International Criminal Law Review,* 1/2021.

Ruan et al.	2023	Machine Learning for fraud	China	Provides review of ML applications in fraud detection, incl. unsupervised anomaly detection models.	Supports tech-focused fraud detection solutions.
Kirkos	2015	DSS & Fraud Risk	Europe	Evaluates decision support systems for fraud detection using AI and statistical methods.	Early insight into predictive fraud modeling.
Zetzsche et al.	2020	DeFi & Crypto Risks	Europe / Global	Outlines how decentralized finance systems create unregulated zones for illicit activity.	Grounds the emerging threat argument within blockchain context.
Weber et al.	2019	Blockchain Forensics	Switzerland	Analyzes blockchain-based tracing methods and transparency models.	Proves effectiveness of blockchain in financial intelligence.
Wischmeyer	2020	AI Ethics & Law	EU	Explores legal admissibility and ethical concerns around black-box AI decision-making in law.	Highlights legal-tech tensions in fraud enforcement.
Sharman	2011	Regulatory Capture	Pacific & Global	Argues that some jurisdictions benefit from weak enforcement ("secrecy havens").	Demonstrates how fraud is facilitated by deliberate under-regulation.
Gillis & Shachar	2022	Data Governance	EU & Israel	Discuss regulatory conflicts between AI/data analytics and privacy law (GDPR).	Frames ethical and data protection challenges of tech solutions.
Bantekas	2021	Multidisciplinary Regulation	Global	Advocates for a fusion of legal, regulatory, and technical efforts in enforcement.	Basis for the review's concluding framework on integrated responses.
Nguyen et al.	2022	AI Adoption Barriers	Vietnam & UK	Highlights barriers to AI adoption in fraud detection: skill gaps, infrastructure, and legal concerns.	Discussion of uneven global capacities in adopting new tools.
Gottschalk	2010	Corporate Crime Framework	Norway	Suggests fraud is a product of both ethical failure and governance breakdown.	Theoretical support for fraud as a systemic governance failure.
Ngai et al.	2011	Big Data in Finance	Hong Kong	Outlines predictive modeling for fraud using big data, AI, and clustering techniques.	Validates potential of scalable predictive tech in large datasets.
Ferwerda et al.	2020	AML Compliance Analysis	EU	Empirical review of AML practices; critiques reliance on banks for frontline enforcement.	Supports the argument of overburdened and fragmented regulatory enforcement.
Basel Committee	2021	AML Supervision	Global Banks	Recommends "risk-based approach" for detecting money laundering in banks.	Important for institutional frameworks and compliance logic.
World Bank	2020	Financial Sector Integrity	Global	Advises financial sector resilience through tech and international cooperation.	Global policy-level reinforcement of the need for integration.

4. METHODOLOGY

This review uses a systematic qualitative methodology to integrate all the interdisciplinary academic researches spanning law, economics, computer science, and regulatory studies, with the aim of providing a comprehensive analysis of global financial fraud and the evolving mechanisms developed to fight it. The approach was designed to find, categorize, and critically evaluate present legal frameworks, regulatory structures, and technological innovations employed in the prevention, detection, and prosecution of financial fraud across different jurisdictions.

4.1. Literature Search Strategy

A thorough and structured literature search was conducted using a range of academic and policy-oriented databases. These included Scopus, Web of Science, Google Scholar, SSRN, and PubMed, as well as specialized legal and institutional repositories such as HeinOnline, LexisNexis, and the OECD iLibrary. The search spanned publications from 2000 to 2024, ensuring inclusion of both foundational texts and recent developments in fraud mitigation strategies.

Search queries combined terms such as: ("financial fraud" OR "economic crime" OR "white-collar crime") AND ("international law" OR "regulatory framework" OR "cross-border enforcement") AND ("machine learning" OR "blockchain" OR "AI" OR "cyber fraud" OR "digital currency").

4.2. Inclusion and Exclusion Criteria

Sources were given preference based on predefined inclusion criteria. Eligible materials included peer-reviewed journal articles, official reports by governmental and intergovernmental bodies, and working papers from recognized research institutions. Literature addressing both traditional financial crimes (e.g., tax evasion, securities fraud) and contemporary threats (e.g., crypto-related scams, cyber-enabled manipulation) was considered.

Only sources offering substantive legal, regulatory, or technological insights into financial fraud detection and enforcement were retained. Exclusion criteria were applied to omit: Non-English publications; Opinion pieces, blogs, or non-scholarly texts lacking analytical or empirical rigor; Redundant studies with no distinctive contribution to thematic analysis.

4.3. Data Extraction and Analysis

The review utilised a narrative synthesis approach. Following an initial screening of 345 documents, 112 were shortlisted for full-text evaluation. Ultimately, 68 texts—including academic articles, legal instruments, and technical

reports—were selected for inclusion based on relevance and analytical depth. Data were categorized across three central dimensions: *Legal Dimension:* having international treaties (e.g., UNCAC, FATF), case law, and legislative interpretations; *Regulatory Dimension:* encompassing national and supranational enforcement rules, compliance frameworks, and institutional mandates; *Technological Dimension:* focusing on new technological advances such as blockchain forensics, AI-driven fraud detection systems, and big data analytics.

Thematic analysis was facilitated through NVivo 14 software, which helped us to identify recurrent legal issues, novel regulatory patterns, and cross-jurisdictional uses of technological tools.

5. RESULTS

5.1. Findings

This review brings forward its perspectives on how financial fraud, from traditional crimes such as insider trading and tax evasion to complex, technology-driven schemes has become widespread. The literature points to the dual role of digital technologies: while improving efficiency, they have introduced exploitable vulnerabilities. Cyber-enabled fraud—including phishing, synthetic identity creation, and cryptocurrency misuse—is now widespread.

It has been noticed how decentralized, under-regulated nature of blockchain systems has especially tracked on being extremely complicated and the tracing of illicit transactions, enabling the cross-border flow of illicit funds with minimal oversight, particularly in regions with weak regulatory frameworks.

Recommendations have come forward to support a degree of global integration in anti-fraud measures. All of it has influenced national policies and increased transparency requirements. However, their implementation remains inconsistent, mostly in third world countries, where infrastructure limitations and legal weaknesses obstruct enforcement. Cross-border fraud also persists as a tough task due to fragmented legal definitions, inconsistent enforcement practices, and difficulties in securing international cooperation and peace.

Some positive outcomes such as regulatory sandboxes and real-time monitoring—are assisting certain countries adapt. Still, divide remains, mostly in areas such as decentralized finance (DeFi) regulation and the analytical ability of financial intelligence units.

Technology is treated as both a key enabler and a challenge in combating fraud. Machine Learning tools for any kind of anomaly detection and blockchain analytics are gaining momentum, yet issues over implementation prices, privacy, algorithmic bias, and legal admissibility of AI-generated evidence persist. Public-private partnerships and collaborative intelligence-sharing models—seen in places like the EU, Singapore, and the UK—offer make sure that they are not yet widely institutionalized.

Overall, the findings reflect that while progression has been made in law, technology, and regulatory awareness, significant gaps persist. An integrated approach where legal reform, technological creation, and international cooperation is important to ensure a more cohesive and effective response to financial fraud.

6. CONCLUSION

This review concludes the complex, rapidly evolving nature of global financial fraud and its intersection with legal, regulatory, and technological domains. International frameworks like the FATF Recommendations and the UNCAC have contributed to greater global alignment, enforcement challenges sustained especially in cross-border contexts.

In advanced economies, regulatory systems are fast and increasingly responsive. Many developing jurisdictions struggle to match the pace of technological change due to limited institutional capacity and resources. The rise of digital finance, such as cryptocurrencies, has multiplied both the scope and sophistication of fraud. Developed and advanced tools offer promising countermeasures, yet raise pressing concerns about privacy, transparency, and the legal status of algorithmic evidence.

Addressing the issue of financial fraud effectively in a digitalized global economy requires well-coordinated action across governments, international bodies, and the private sector. The need of the hour is to build institutional resilience, harmonizing legal standards, and investing in technological infrastructure will be essential to safeguarding financial integrity, promoting economic stability, and preserving public trust.

Please Note: The author utilized AI-assisted tools to support the organization and synthesis of literature; most of the interpretations, critical evaluations, and conclusions reflect original scholarly analysis.

BIBLIOGRAPHY

Arner D. W., Barberis J., Buckley R. P., "The evolution of fintech: A new post-crisis paradigm?", *Georgetown Journal of International Law,* 47/2016.

Bantekas I., "A unified approach to transnational criminal enforcement: Beyond mutual legal assistance" *International Criminal Law Review,* 1/2021.

Basel Committee on Banking Supervision, *Sound management of risks related to money laundering and financing of terrorism,* Bank for International Settlements, 2021, https://www.bis.org/bcbs/publ/d505.pdf, 30 April 2021.

Button M., Johnston L., Frimpong K., Smith G., "Fraud and its relationship to technological advancement", *Journal of Financial Crime,* 1/2022.

Ferwerda J., Deleanu I., Unger B., "Strategies to avoid blacklisting: The case of statistics on money laundering", *European Journal on Criminal Policy and Research,* 4/2020.

FATF, *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations,* Financial Action Task Force, 2023 https://www.fatf-gafi.org, 30 April 2025.

Gillis T., Shachar C., "Artificial intelligence and the GDPR: Navigating the regulatory and ethical minefields", *Computer Law & Security Review,* 44/2022.

Gottschalk, P., *Policing financial crime: Intelligence strategy, implementation and organizational change,* CRC Press, 2010.

Kirkos E., "Assessing corporate fraud risk with decision support systems: A review", *European Journal of Operational Research,* 1/2015.

Levi M., Reuter P, "Money laundering", *Crime and Justice,* 34/2006.

Nguyen T. T., Nguyen Q. U., Nguyen T. H., "Barriers to adopting artificial intelligence in financial fraud detection: A cross-national study", *Information Systems Frontiers*, 24/2022.

OECD, *Fighting tax crime: The ten global principles* (2nd ed.), OECD Publishing, 2023.

Ruan Y., Wu J., Zhang Y., "Using machine learning for financial fraud detection: A systematic literature review", *Expert Systems with Applications,* 212/2023.

Sharman J. C., *The money laundry: Regulating criminal finance in the global economy,* Cornell University Press, 2011.

Unger B., Ferwerda J., *Money laundering in the real estate sector: Suspicious properties,* Edward Elgar Publishing, 2011.

Weber R. H., Staiger D., Schwarz A., "Blockchain-based tracing: Applying blockchain technology for tracking and tracing products in supply chains", *Journal of Law, Information and Science,* 2/2019.

Wischmeyer T., "Artificial intelligence and transparency: A blueprint for improving the regulation of AI", *German Law Journal,* 2/2020.

World Bank, *Enhancing financial integrity: Global trends and challenges*, 2020, https://www.worldbank.org/en/topic/financialsector/publication, 30 April 2025.

Zetzsche D. A., Buckley R. P., Arner D. W., Barberis, J. N., "Decentralized finance (DeFi)", *Journal of Financial Regulation,* 2/2020.

LEGAL SOURCES

UNODC. (2004). *United Nations Convention against Corruption.* United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/corruption/convention.html, 30 April 2025.

Sanjeev P. Sahni, PhD*

НАУЧНИ ПРИСТУП БОРБИ ПРОТИВ ГЛОБАЛНИХ ФИНАНСИЈСКИХ ПРЕВАРА: ПРАВНИ, РЕГУЛАТОРНИ И ТЕХНОЛОШКИ АСПЕКТИ

Резиме

Апстракт: *Финансијске преваре остају озбиљан глобални проблем који превазилази државне границе, слаби финансијске системе и доприноси економској нестабилности. Ова студија анализира финансијске преваре кроз научну призму, истичући сложеност њихових механизама и све променљивије изазове које представљају за међународно право и регулаторне оквире. Рад настоји да категоризује преваре на традиционалне финансијске криминале, као што су манипулације хартијама од вредности, утаја пореза и инсајдерска трговина, као и на нове претње као што су сајбер преваре, дигиталне валуте и децентрализовани финансијски системи. Циљ је и да се процени ефикасност међународних правних инструмената, као што су препоруке Радне групе за финансијску акцију (FATF), Конвенција Уједињених нација против корупције (UNCAC) и регионалне споразуме, у откривању, спречавању и гоњењу финансијских превара. Поред тога, студија испитује употребу напредних технолошких алата, укључујући машинско учење, анализу података и блокчејн форензику, у откривању и превенцији финансијских превара. Помоћу квантитативних студија случаја и емпиријских података, рад пружа увиде у ефикасност постојећих правних мера и предлаже нове, научно засноване методологије за унапређење глобалне борбе против финансијских превара. Закључак наглашава потребу за адаптивним, холистичким оквиром који обједињује правне, научне и технолошке ресурсе за ефикаснију борбу против финансијских превара у све сложенијој глобалној економији.*

Кључне речи: финансијске преваре, транснационални криминал, међународна регулатива, блокчејн форензика, децентрализоване финансије (DeFi).

* Еминентни професор, оснивач и генерални директор „Sumona Institute of Behavioral Sciences“, Њу Делхи, Индија, drspsahni@gmail.com.