

Received: 11 December 2025

Revised: 25 February 2026

Accepted: 9 March 2026

COMBATING MONEY LAUNDERING: APPLYING ARTIFICIAL INTELLIGENCE TO DETECT SUSPICIOUS MUTUAL FUND TRANSACTIONS

Anupa ROJANASOONTRA¹ and Sumonthip CHITSAWANG¹¹ Faculty of Political Science, Chulalongkorn University, Thailand;

anupa.roj@gmail.com (A. R.); sumonthip99@hotmail.com (S. C.)

Handling Editor:

Professor Dr. Muhammad HASEEB

VIZJA University, Poland

(This article belongs to Theme 1: Humanities & Social Sciences for Sustainability)

Reviewers:

1) Professor Dr. Attapol KUANLIANG

Midwestern State University, USA.

2) Assistant Professor Dr. Supatra PHANWICHIT

STOU, Thailand

3) Police Major General Dr. Thanarat SONKLA

Narcotics Suppression Bureau, Thailand

Abstract

This qualitative study examines complex money-laundering patterns in the asset management industry and explores strategic guidelines for applying Artificial Intelligence (AI) to detect suspicious mutual fund transactions. Utilizing in-depth, semi-structured interviews with twenty-one purposively selected key informants—comprising compliance officers at asset management companies and regulatory authorities from the Anti-Money Laundering Office—the research systematically analyzes current financial crime vulnerabilities. The empirical findings reveal that illicit funds are typically laundered through systematic placement, concealment, and economic integration within mutual fund portfolios. While AI offers a transformative solution for identifying anomalous financial behavior and effectively cross-referencing watchlist individuals, significant operational challenges remain. Consequently, the study proposes a comprehensive implementation framework that emphasizes seven critical guidelines: establishing clear corporate policies, managing employee adaptation to new technology, optimizing budget allocations, ensuring strict data privacy, acknowledging inherent algorithmic limitations, evaluating overall cost-effectiveness, and reinforcing rigorous compliance oversight. Ultimately, intelligently integrating AI into anti-money laundering protocols significantly enhances transaction monitoring efficiency, fortifying the financial sector against increasingly sophisticated economic crimes while safeguarding long-term market sustainability and promoting broader economic security.

Keywords: Economic Crime, Anti-Money Laundering, Artificial Intelligence, Suspicious Transaction Monitoring, Mutual Fund Governance

Citation Information: Rojanasoontra, A., & Chitsawang, S. (2026). Combating Money Laundering: Applying Artificial Intelligence to Detect Suspicious Mutual Fund Transactions. *Asian Interdisciplinary and Sustainability Review*, 15(1), Article 11. <https://doi.org/10.14456/aisr.2026.11>

Introduction

Money laundering severely undermines global economic stability and social development by disguising illicit profits generated from transnational crimes (Ngamkaiwan et al., 2016). The scale of this shadow economy is staggering; the Tax Justice Network (2020) estimates that between \$21 trillion and \$32 trillion in private assets are concealed in global tax havens, with illicit cross-border capital flows significantly dwarfing international aid budgets. In Thailand, this crisis persists despite robust enforcement of the Anti-Money Laundering Act of 1999, as shown by a steady annual increase in asset seizure orders that culminated in the confiscation of over 9.39 billion baht in 2023 alone (Anti-Money Laundering Office, 2023). Increasingly, sophisticated criminals are exploiting legitimate financial vehicles, such as mutual funds, which pool public savings for varied securities investments managed by asset management companies (AMCs) (Land and Houses Fund Management Co., Ltd., 2023).

As the financial sector transitions into the digital age, AMCs have widely adopted electronic Know Your Client (e-KYC) and Client Due Diligence (CDD) procedures to verify customer identities, assess financial status, and ensure regulatory compliance (Securities and Exchange Commission, 2023a). While these digital channels offer unprecedented convenience and accessibility, they concurrently expose financial institutions to advanced fraudulent vulnerabilities (Bank of Thailand, 2023). Despite stringent regulations governing technology use in KYC processes, money laundering techniques have become highly sophisticated, with criminals increasingly channeling illicit funds into mutual funds through bond investments or holding statements (Securities and Exchange Commission, 2023b). The Thailand Development Research Institute (2021) highlights that current regulatory frameworks struggle to keep pace with these evolving, high-stakes economic crimes, underscoring the urgent need for more dynamic and responsive risk assessment mechanisms within the asset management industry.

To effectively counteract these multidimensional threats, Artificial Intelligence (AI) has emerged as a transformative solution capable of analyzing vast datasets with unprecedented speed and precision (Leepipatpaiboon & Lertmethapat, 2019). The financial services sector is rapidly adopting AI for both front-office customer analytics and back-office compliance functions, including the critical detection of fraudulent or suspicious transactions (KPMG, 2022; Mingsakul, 2023). By deploying advanced predictive models and identity verification systems, AMCs can significantly enhance their capacity to verify the legitimacy of financial transactions and prevent mutual funds from being exploited as money-laundering conduits (Indhrakaset et al., 2023). Consequently, this qualitative study systematically examines contemporary money laundering patterns within mutual funds, critically evaluates the operational challenges of integrating AI for transaction monitoring, and proposes strategic guidelines to optimize AI implementation for detecting suspicious financial activities.

Literature Review

Theory of Economic Crimes

Economic crimes exact a substantially higher toll on society than traditional offenses because they inherently destabilize overarching economic systems through corporate fraud, corruption, embezzlement, and market manipulation (Lilly et al., 2014). Unlike conventional criminals, the perpetrators are frequently highly educated, reputable professionals and corporate executives who weaponize their socio-economic status, specialized knowledge, and powerful networks to orchestrate sophisticated, non-violent schemes (Siegel, 2013). By exploiting systemic legal loopholes and leveraging their professional credibility, these offenders successfully conceal illicit activities, misappropriate assets, and evade detection, prioritizing immense financial gain over public well-being. Consequently, while these transgressions—variously termed white-collar, corporate, or financial crimes—rarely involve physical violence, their cumulative impact profoundly threatens national economic security, eroding institutional

integrity and victimizing both governmental agencies and the broader public (Lilly et al., 2014; Siegel, 2013).

Conceptual Foundations and Learning Processes of Artificial Intelligence

Artificial Intelligence (AI) represents a transformative technological paradigm that engineers computational systems, machinery, and electronic devices to replicate human intellect, enabling sophisticated problem-solving, rational decision-making, and data-driven forecasting (Goodfellow et al., 2016; Janiesch et al., 2021). At its core, AI analyzes vast, complex datasets to identify underlying patterns, allowing systems to independently execute tasks that traditionally require human cognitive abilities, such as perception, comprehension, and reasoning (Russell & Norvig, 2021). This functional capacity is deeply rooted in a machine learning process that mirrors human cognition—encompassing data recognition, contextual understanding, and adaptive response mechanisms. To maximize AI's operational efficacy, organizations must carefully select appropriate algorithmic models, continuously feed them with expansive, high-quality datasets, and rigorously monitor their internal mechanisms. Through this continuous cycle of data assimilation and performance tuning, AI systems incrementally improve predictive accuracy, ultimately enabling institutions to make precise, policy-level decisions with unprecedented efficiency and reliability.

The Application of AI in Asset Management

Russell & Norvig (2021) outline the working process of AI in seven stages: 1) Data Collection; 2) Data Understanding and Conversion; 3) Model Selection and Creation; 4) Model Training and Tuning; 5) Testing and Evaluation; 6) Improvement and Operation; and 7) Continuous Learning and Improvement. This process enables AI to learn and adapt to changing data and circumstances, allowing it to perform intelligent decision-making tasks as required.

For asset management companies (AMCs), leveraging advanced computational processing is essential for detecting suspicious mutual fund transactions (Janiesch et al., 2021). This technological ecosystem encompasses foundational Artificial Intelligence (AI), which enables systems to analyze, plan, and make rapid, precise decisions; Machine Learning (ML), which allows computers to identify patterns and improve predictive performance without explicit programming; and Deep Learning (DL), which processes complex information through multilayered neural representations to generate sophisticated outputs. Driven by the exponential growth of electronic data and high-performance computing, these technologies enable capital market firms to systematically monitor organizational risks, detect irregularities, and optimize customer service through data-driven investment strategies (Securities and Exchange Commission, 2023a). Correspondingly, the Financial Industry Regulatory Authority (2020) reports that global financial institutions are allocating substantial resources to AI-driven applications. These applications primarily use natural language processing to enhance customer experiences via virtual assistants, deploy predictive analytics for precision portfolio management, and, critically, employ robust pattern-recognition algorithms within Know Your Client (KYC) processes to flag anomalous behaviors and prevent sophisticated financial crimes.

Research Conceptual Framework

This study's conceptual framework synthesizes the multifaceted dynamics of detecting suspicious mutual fund transactions. As illustrated in Figure 1, the framework is grounded in the relevant legal infrastructure, notably the Anti-Money Laundering Act of 1999 and established regulatory guidelines for Customer Due Diligence (CDD) and electronic Know Your Customer (e-KYC) processes. It outlines the main motivations driving criminals to exploit mutual funds—such as high potential returns and the ease of online account management—alongside the major operational obstacles regulators face. These vulnerabilities include clients actively concealing information, the sheer volume and velocity of investment transactions, and the absence of standardized criteria for flagging anomalies. Ultimately, this

framework shows how integrating Artificial Intelligence can bridge these gaps, significantly improving the effectiveness of KYC and CDD protocols in identifying suspicious individuals before they enter legitimate investment channels.

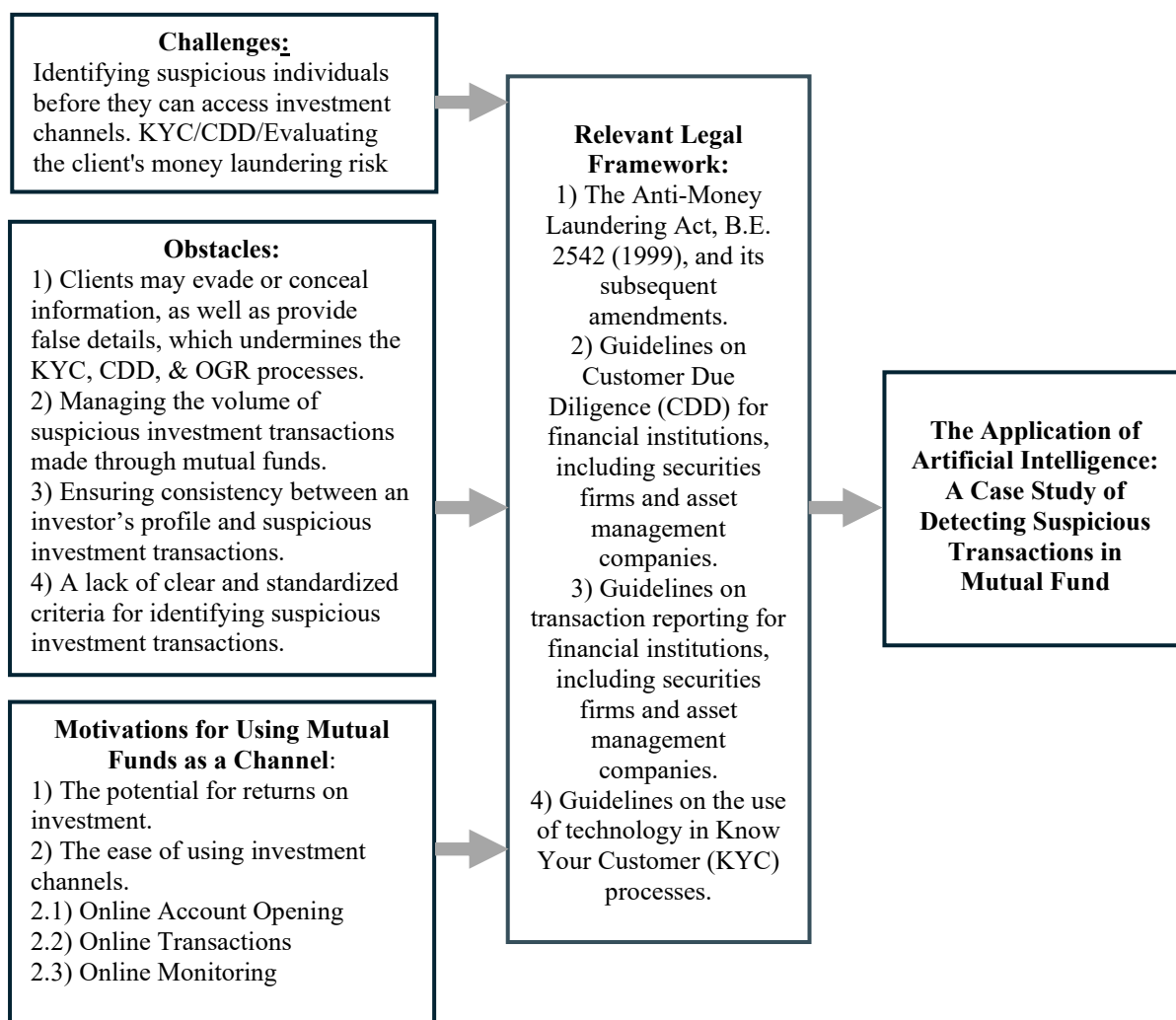


Figure 1 Research Conceptual Framework

Research Methodology

To systematically investigate the application of Artificial Intelligence in detecting suspicious mutual fund transactions, this study employed a qualitative research design utilizing in-depth, semi-structured interviews. The research sample comprised twenty-one key informants, purposively selected to ensure deep institutional insight; these included compliance officers and asset management professionals, as well as government regulators from the Anti-Money Laundering Office. Before data collection, the researchers strictly observed all ethical protocols for human subjects and obtained informed consent for comprehensive audio and photographic recordings. The researchers then subjected the primary qualitative data from these targeted interviews to rigorous content analysis. This systematic approach enabled the researchers to categorize qualitative insights according to the core thematic objectives, exclude irrelevant data, and synthesize robust, empirically grounded conclusions on current money-laundering patterns, technological challenges, and strategic AI implementation guidelines.

Research Findings

Patterns of Money Laundering within Mutual Funds

The empirical investigation reveals that money laundering within mutual funds functions as a sophisticated mechanism to disguise illicit profits generated from severe criminal activities, including arms trafficking, the drug trade, prostitution, securities fraud, and deceptive foreign exchange scams. Driven by the need to legitimize enormous illicit profits, criminals systematically exploit the financial system through a three-stage laundering process. First, criminals introduce illicit capital into the financial system, then deliberately obscure its origin through complex layering techniques. Ultimately, they reintegrate these funds into the legitimate economy, allowing criminals to use the money under the guise of legitimate investment returns or proceeds from high-value asset liquidations.

Operational Challenges in Suspicious Transaction Monitoring

While Artificial Intelligence offers transformative potential for detecting these illicit flows, asset management companies (AMCs) face significant operational challenges in its application. Specifically, compliance officers struggle with effectively monitoring transactions that subtly deviate from a client's documented economic status and historical financial data. They also face major technical difficulties accurately identifying nuanced investment behaviors that warrant suspicion without disrupting normal operations. This complexity is exacerbated by the need to seamlessly cross-reference real-time transactions against individuals under government investigation, as well as to rapidly identify transactions executed by persons recently flagged in adverse public news and mass media reports.

A Strategic Framework for AI Implementation

To systematically overcome these vulnerabilities, the findings propose a comprehensive, seven-point framework for implementing AI in suspicious transaction monitoring. First, executive management must establish clear corporate policies and practical guidelines to build organizational understanding and encourage technology adoption. Second, this must be paired with proactive change management, utilizing executive support to help employees across all departments adapt to new operational paradigms. Third, AMCs must optimize their budgets by adopting cost-effective AI programs specifically tailored to the needs of their support and operations units. Fourth, firms must enforce strict data privacy and security protocols, ensuring analytical processes do not violate personal privacy or harm customer sentiment. Fifth, organizations must acknowledge AI's inherent algorithmic limitations and continuously verify its outputs to mitigate factual inaccuracies, latency, or the system's inability to process human emotional contexts. Sixth, organizations must thoroughly assess the technology's overall cost-effectiveness and necessity to prevent inefficient resource depletion. Finally, all AI deployments must be strictly supervised to ensure alignment with established compliance standards and governance frameworks in the asset management business.

Conclusion and Discussion

Exploitation of Asset Management by Criminal Syndicates

Criminals increasingly exploit the asset management industry not to commit predicate offenses, but as sophisticated vehicles for laundering illicit proceeds through complex property transfers and layering. Because AMCs serve as the ultimate destination for these funds, they are highly vulnerable to being used as conduits for integrating illicit cash into the legitimate economy, a risk exacerbated by the industry's rapid transfer speeds, complex transaction structures, and expert client base.

Navigating the Organizational Challenges of AI Integration

While implementing AI offers a transformative solution for monitoring these high-volume transactions and improving decision-making, it also introduces substantial organizational challenges. Transitioning to AI requires a challenging adjustment period that can temporarily

reduce operational efficiency and increase work-related anxiety among employees (Bridges & Bridges, 2017). Successfully operationalizing AI to detect anomalous financial behaviors requires a strategic, multifaceted approach championed by executive management. Clear corporate policies ensure smooth budget allocation and give compliance units a clear mandate to shift from vulnerable rule-based methods to advanced predictive analytics (Hidayat et al., 2024; Oztas et al., 2024). While full-scale implementation brings heavy financial burdens, AMCs can maximize benefits by strategically deploying cost-effective AI tools within their support and fund operations units, boosting efficiency, reducing human error, and improving fraud detection by up to 20% (Svoboda, 2023). Crucially, this technological integration demands profound employee adaptability. Although younger demographics increasingly view AI as indispensable, approximately 37% of organizations remain unprepared for this workforce transition (Deloitte Global, 2025). Therefore, leaders must implement robust change management strategies that enhance employee autonomy and team productivity (Ali & Badi, 2022) while ensuring personnel receive the training needed to retain a central, balanced role in critical decision-making processes (Mardyan & Noknoi, 2024; Trunk et al., 2020).

Safeguarding Data Privacy and Mitigating Algorithmic Risks

As financial institutions collect vast amounts of sensitive data, they become prime targets for global criminal syndicates, so AI deployments must prioritize data privacy and security to prevent breaches and maintain customer trust (Alhajeri & Alhashem, 2023). Navigating these obstacles requires cultivating a culture of innovation, investing in standardized data governance, and ensuring that AI analysis does not inadvertently harm customer sentiment or violate personal privacy (Rane et al., 2024). Furthermore, organizations must critically acknowledge AI's inherent algorithmic limitations, including potential factual inaccuracies, data latency, and the inability to process human emotional contexts. To mitigate these risks, AI applications require strict regulatory oversight, such as the European Union's (2024) Artificial Intelligence Act, which categorizes systems by risk levels, and Singapore's Monetary Authority frameworks, which emphasize regulatory sandboxes and individual accountability for senior managers to deter misuse. Effective AI deployment ultimately relies on robust corporate risk management, rigorous information security protecting data confidentiality and integrity, and highly skilled personnel capable of overseeing these complex systems (Duan et al., 2019; Gupta et al., 2023; Muandej, 2023; Securities & Exchange Commission, 2023a).

Actionable Policy Recommendations and Future Research

To operationalize these strategic guidelines, AMC executives should develop comprehensive implementation plans that encompass policy setting, employee adaptation, budget optimization, data security, and rigorous compliance supervision. Actionable steps include proactively recruiting AI-proficient personnel while simultaneously upskilling existing staff to foster a hybrid workflow that seamlessly integrates human judgment with artificial intelligence. By prioritizing active listening, collaborative learning, and transparent change management with all stakeholders, institutions can maximize the efficacy of suspicious transaction monitoring for both the organization and its workforce. Building upon this conceptual framework, future research should explore the specific impacts of AI on detecting anomalies within listed securities on the Stock Exchange of Thailand, thereby continuously refining the technological defenses of the broader capital market.

References

- Alhajeri, R., & Alhashem, A. (2023). Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management*, 15(4), 284-305.
- Ali, A., & Badi, S. (2022). Exploring the Impacts of Artificial Intelligence (AI) Implementation at Individual and Team Levels: A Case Study in the UAE Government Sector. In M.

- Themistocleous & M. Papadaki. (eds.). *Information Systems* (pp. 597-613). Cham: Springer.
- Anti-Money Laundering Office. (2023). *Annual Report 2023*. Bangkok: Anti-Money Laundering Office.
- Bank of Thailand. (2023). *Policy on managing financial transaction fraud*. Bangkok: Bank of Thailand.
- Bridges, W., & Bridges, S. (2017). *Managing Transitions: Making the Most of Change*. Massachusetts: Nicholas Brealey Publishing.
- Deloitte Global. (2025). *Gen Z and Millennial Survey 2025*. Retrieved from www.deloitte.com/content/dam/assets-shared/docs/campaigns/2025/2025-genz-millennial-survey.pdf.
- Duan, Y., Edwards, J., & Dwivedi, Y. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda. *International Journal of Information Management*, 48, 63-71.
- European Union. (2024). *EU Artificial Intelligence Act*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. Massachusetts: MIT Press.
- Gupta, D., Miryala, N., & Srivastava, A. (2023). Leveraging Artificial Intelligence for Countering Financial Crimes. *International Journal of Artificial Intelligence & Machine Learning*, 2(1), 103-120.
- Hidayat, H., Ardi, Z., Ahlunnazak, A., Harmanto, D., Orji, C., & Isa, M. (2024). Determining the influence of digital literacy on learning personal competence: The moderating role of Fear of Missing Out. *European Journal of Educational Research*, 13(4), 1775-1790.
- Indhrakaset, S., Nimmual, N., & Gasondokmai, W. (2023). Application of artificial intelligence in financial management in Thailand. *Journal of the Association of Researchers*, 28(4), 73-87.
- Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, <https://doi.org/10.48550/arXiv.2104.05314>.
- KPMG. (2022). *Transparency Report 2021*. Retrieved from <https://assets.kpmg.com/content/dam/kpmgsites/qa/pdf/2022/09/transparency-report-2021.pdf.coredownload.inline.pdf>.
- Land and Houses Fund Management Co., Ltd. (2023). *LH Japan Government Bond Fund 3MI Factsheet*. Bangkok: Land and Houses Fund Management Co., Ltd.
- Leepipatpaiboon, P., & Lertmethapat, N. (2019). *Artificial Intelligence in Thailand: Case Study in Financial Services*. Bangkok: Bank of Thailand.
- Lilly, J., Cullen, F., & Ball, R. (2014). *Criminological Theory: Context and Consequences* (6th ed.). California: SAGE Publications.
- Mardyan, W., & Noknoi, C. (2024). The Impact of Artificial Intelligence (AI) on Organizational Culture and Employee Relationships in the Credit Department: A Case Study of a Financial Institution. *Journal of Roi Kaensarn Academi*, 9(11), 620-631.
- Mingsakul, P. (2023). *Tech Trends in the Banking Sector in 2023*. Retrieved from www.krungsri.com/en/research/research-intelligence/tech-trend-2023.
- Muandej, N. (2023). *Factors Influencing the Adoption of AI Technology in Accounting Practices of Accountants in Bangkok: A Case Study of ChatGPT*. Master of Business Administration Thesis, Thammasat University.
- Ngamkaiwan, C., Sirivunnabood, P., Borwornnuntakul, T., & Lerdtomornsakul, U. (2016). Problems of money laundering within foreign banks in Thailand affecting the confidence of foreign investors. *Journal of Thai Justice System*, 9(1), 83-105.
- Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future Generation Computer Systems*, 159, 161-171.

- Rane, N., Choudhary, S., & Rane, J. (2024). *Acceptance of artificial intelligence technologies in business management, finance, and e-commerce: Factors, challenges, and strategies*. Retrieved from <http://dx.doi.org/10.2139/ssrn.4842268>.
- Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). London: Pearson.
- Securities and Exchange Commission. (2023a). *Guideline on the application of Artificial Intelligence and Machine Learning in the capital market*. Bangkok: Securities and Exchange Commission.
- Securities and Exchange Commission. (2023b). *Guideline on the application of technology to KYC*. Bangkok: Securities and Exchange Commission.
- Siegel, L. (2013). *Criminology: Theories, Patterns, and Typologies* (11th ed.). Kentucky: Wadsworth Cengage Learning.
- Svoboda, A. (2023). The Impact of Artificial Intelligence on the Banking Industry. *Journal of Banking and Finance Management*, 4(1), 7-13.
- Tax Justice Network. (2020). *Financial Secrecy Index 2020 reports progress on global transparency – but backsliding from US, Cayman and UK prompts call for sanctions*. Retrieved from <https://taxjustice.net/press/financial-secrecy-index-2020-reports-progress-on-global-transparency-but-backsliding-from-us-cayman-and-uk-prompts-call-for-sanctions/>.
- Thailand Development Research Institute. (2021). *Trends in money laundering in Thailand: A case study of money laundering through juristic persons and front businesses, lawyers and accountants, tour operators, foreign trusts operating in Thailand, fraudulent rotating savings and credit associations, and money laundering through non-profit organizations*. Retrieved from <https://tdri.or.th/2021/12/research-study-on-trends-of-money-laundering-2/>.
- The Financial Industry Regulatory Authority. (2020). *Artificial Intelligence (AI) in the securities industry*. Retrieved from www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf.
- Trunk, A., Birkel, H., & Hartmann, E. (2020). On the current state of combining human and artificial intelligence for strategic organizational decision making. *Business Research*, 13, 875-919.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or a claim that its manufacturer may make, is not guaranteed or endorsed by the publisher.



Copyright: © 2026 by the authors. This is a fully open-access article distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).