JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i3

The Typology of Banking Crimes in the Disruptive Era: A Comprehensive Review of Criminal Modi Operandi and Law Enforcement Challenges

Ruslan Mustari
Fakultas Hukum Universitas Bosowa, Makassar, Indonesia, ruslanmustari@universitasbosowa.ac.id.

Corresponding Author: ruslanmustari@universitasbosowa.ac.id

Abstract: Banking crime is a global phenomenon that continuously mutates alongside technological disruption and economic dynamics. This article presents a comprehensive review of banking crime typologies through a conceptual and analytical approach to current academic literature. The focus of the study encompasses the constellation of money laundering, banking fraud, cybercrime, white-collar crime, terrorism financing, and corruption. The synthesis results indicate that criminal modi operandi have radically transformed, shifting from traditional models to the exploitation of regulatory loopholes (regulatory arbitrage), trade-based money laundering (TBML), the exploitation of money mules, and the abuse of digital instruments. Conversely, the primary challenges in law enforcement include regulatory lag, the borderless evolution of criminal technology, and institutional reluctance to report internal fraud to preserve corporate reputation. This review asserts that a comprehensive understanding of crime typologies is a fundamental prerequisite for formulating effective policies. Therefore, holistic legal reform is recommended through a shift toward a risk-based supervisory framework, the strengthening of the corporate criminal liability doctrine, and the mandated adoption of integrated RegTech and SupTech to secure the stability of the national financial architecture.

Keyword: Banking Crime, Money Laundering, Cybercrime, Compliance, Banking Law.

INTRODUCTION

Banking crime is a global phenomenon that continues to evolve in tandem with technological disruption, regulatory changes, and macroeconomic dynamics. Banking institutions, as the heart of the modern financial system, are not only targets of crime but are also frequently exploited as the primary means or instruments for laundering the proceeds of criminal activity. As business models shift toward digital banking which operates almost entirely beyond jurisdictional boundaries the complexity of the threats faced by this sector has escalated to unprecedented levels. This situation compels stakeholders, including both regulators and banking practitioners, to continuously and periodically evaluate their security and legal compliance frameworks.

Conceptually, financial and banking crimes are defined as the unlawful conversion or acquisition of property or assets belonging to another party for personal use and gain. These crimes are fundamentally criminal acts motivated by the pursuit of financial gain (Tripathi & Tripathi, 2023). Within the banking landscape, the spectrum of these crimes is highly heterogeneous, encompassing money laundering, fraud, embezzlement, cybercrime, and various other forms of white-collar crime (Gavrilko, 2020; Shonhadji, 2020). Perpetrators range from independent individuals and transnational organized crime groups to internal actors or corporate banking elites who exploit their positions.

Among these various forms of crime, money laundering remains the most massive and systemic form of banking crime. At its core, money laundering is a practice of disguise where the proceeds of crime are infiltrated into financial institutions to appear as a series of legitimate business transactions (Patel et al., 2023b). Although the traditional three-stage model placement, layering, and integration remains the foundational framework, various studies indicate that this practice has evolved rapidly. Modus operandi have now transformed into trade-based money laundering (TBML), the exploitation of money mules, and the use of the under-documented economy and virtual assets (Irwin et al., 2012; Sultan & Mohamed, 2024; Tiwari et al., 2025).

In addition to money laundering, the modern banking sector also faces increasingly disruptive threats of fraud and cybercrime. Banking fraud is no longer limited to traditional loan manipulation or internal embezzlement (Alba, 2000), but has expanded into cybercrimes such as social engineering, identity theft, and point-of-sale manipulation (Cotoc et al., 2021; Williams, 2007). Rapid digital transformation also creates opportunities for the emergence of transaction laundering, where digital payment ecosystems are misused to mix funds from illegal business entities with transactions from legitimate merchants (Saxena, 2024).

Furthermore, the banking system is often entangled in the intersection of various transnational crimes and extraordinary crimes, particularly corruption and terrorist financing. Corruption and bribery—especially those involving Public Officials or Politically Exposed Persons (PEPs)—constitute one of the primary "predicate offenses" that taint the banking system, particularly in developing countries (Sultan & Mohamed, 2024). On the other end of the spectrum, terrorist financing exploits the financial system not through massive volumes of funds, but through highly sophisticated camouflage techniques—such as the misuse of nonprofit organizations—to maintain absolute anonymity and evade the authorities' radar (Patel et al., 2023b).

Faced with such a complex constellation of crimes, prevention and law enforcement efforts in the banking sector still frequently hit dead ends. There is a significant gap between static legislative and risk management frameworks and the pace of innovation in white-collar criminals' tactics. In practice, law enforcement officials are often hindered by limited technical knowledge regarding the complex business processes of banking and capital markets (Bintoro et al., 2020). Furthermore, there is a pattern of reluctance on the part of banking institutions themselves to report incidents of internal or cyber fraud, solely due to concerns about reputational damage and the loss of public trust (Alba, 2000).

Given the escalation of these threats and regulatory gaps, a comprehensive understanding of the typology of banking crimes is an absolute prerequisite for formulating responsive legal policies and compliance systems. This typology serves as a set of essential "red flags" for financial institutions, compliance analysts, and law enforcement officials. Therefore, this article aims to present a systematic review of banking crime typologies based on a synthesis of the latest academic literature, in order to map out modus operandi, identify weaknesses in existing systems, and formulate theoretical recommendations to strengthen the banking legal framework in the face of modern criminal threats.

METHOD

This article employs a normative legal research method with a conceptual approach and an analytical approach to various bodies of literature. The primary data source is a systematic literature review of reputable international and national journals that discuss the typology of financial and banking crime. Secondary data are analyzed qualitatively to identify patterns, classifications, and legal gaps in the handling of banking crime.

RESULTS AND DISCUSSION

Money Laundering as the Epicenter of Crime

Money laundering constitutes the most significant and complex form of banking crime, frequently embedded within organized criminal activities such as extortion, human trafficking, and corruption. In essence, it is a practice whereby the proceeds of crime are disguised as legitimate transactions upon entering financial institutions. Money laundering is classified as a financial crime that can be embedded in organized criminal activity, including robbery, extortion, embezzlement, fraud, human trafficking, and various other offenses. The typologies of money laundering describe the various media, tactics, strategies, practices, schemes, and mechanisms used by criminals to disguise, launder, or move the proceeds of crime. These typologies constitute a series of indicators or red flags that must be observed when banks and financial services institutions carry out their compliance duties (Tripathi & Tripathi, 2023).

In its development, a dynamic tension exists between traditional and contemporary money laundering models. Although the traditional placement-layering-integration model remains relevant, its application now exhibits notable limitations. Irwin et al. (2012) found that the use of an increasing number of techniques correlates directly with the success of money laundering; the more techniques employed, the more cash can be successfully laundered or concealed (Shonhadji, 2020); . However, Sultan and Mohamed highlighted that in less documented economies such as those in South Asia, traditional typologies have shifted toward cash smuggling, round-tripping, and the *hawala* system. Their study found that primary predicate offenses include corruption, tax crimes, smuggling, and drug and human trafficking, and that Pakistani launderers often use traditional typologies including cash smuggling, round-tripping, multiple bank accounts, investment in real estate, and *hawala* (Gavrilko, 2020). In line with this, Menz (2019) also criticized the excessive focus on the three-stage model, arguing that the perception of trade-based money laundering in the financial services sector is overly focused on placement, layering, and integration, while the full extent of the offense under the Proceeds of Crime Act 2002 is less well known. Financial services firms need to improve their understanding of the nature of trade-based money laundering under UK law (Patel et al., 2023b).

In response to these dynamics, the principal typologies of money laundering within the banking system continue to evolve into various modi operandi. The most fundamental practice is *structuring* or *smurfing*—the breaking down of large transactions into smaller portions to avoid reporting thresholds. Structuring has become a global phenomenon in the context of financial crime, and compliance managers who possess awareness of structuring techniques may be able to revise their financial crime risk management frameworks to effectively detect money laundering activities within their financial institutions (Patel et al., 2023b). Furthermore, the use of multiple accounts and anomalous cash deposits continues to dominate suspicious activity reports, as identified in trends in Albania (Levi & Reuter, 2006) and Pakistan (Gavrilko, 2020). In Albania, significant cash deposits in banks without a known source constituted one of the most common typology forms, accounting for 13% of suspicious activity reports (Levi & Reuter, 2006). On the other hand, due to the tightening of surveillance on the pure banking system, criminal actors have increasingly shifted to trade-based money laundering (TBML) modes, using shell companies and manipulating trade values (Irwin et al.,

2012; Patel et al., 2023b). Tiwari et al. (2025) found that the focus placed on the financial system by government agencies and organizations such as FATF, banks, and other financial institutions has increased the likelihood of detecting the laundering of illicit funds, which has consequently led perpetrators to shift to money laundering typologies outside the financial system, particularly TBML. TBML has been described through studies focusing on the use of bank networks, shell companies, and trade operations at free ports (Irwin et al., 2012).

Another increasingly prevalent modus is the exploitation of *money mules*, whereby perpetrators exploit the accounts of vulnerable groups—such as the elderly and students—to layer the movement of stolen funds. Money mules are used by organized criminal groups or fraudsters to launder illicit funds from criminal activities; they allow their accounts to be used for money laundering, and the attacker would layer the stolen funds using money mule accounts. Vulnerable individuals such as the elderly, students, immigrants, and widows are recommended to undergo stricter account opening and account monitoring processes, especially in dealing with remittances, large cash deposits, and rapid fund movements (Sultan & Mohamed, 2024).

Moreover, these criminal schemes are no longer confined to conventional banks but have massively exploited the non-bank sector. This is evidenced by the high incidence of money laundering through capital markets (Menz, 2019); the abuse of non-profit organizations (Ibraj, 2016; Tripathi & Tripathi, 2023), and the expanding use of digital instruments such as virtual assets and online casinos (Tiwari et al., 2025). Bintoro et al. (2020) found that the Indonesian capital market is at high risk of being used as a means of laundering corrupt money, and that a major obstacle arises when investigators and prosecutors handle money laundering cases conducted in the capital market because they have not had enough knowledge related to the capital market and its business processes (Menz, 2019). Naheem (2018) noted that charitable organizations have been known to be used to facilitate terrorism-related activities, and their role in supporting non-terrorist money laundering is also an increasingly documented issue (Ibraj, 2016). Koval identified the legalization of funds using virtual currencies and online casinos as increasingly developing money laundering schemes and methods (Tiwari et al., 2025).

Based on the exposition of these dynamics and typologies, it can be analyzed that the evolution of money laundering reflects a phenomenon of "regulatory arbitrage" that is systematically exploited by criminal actors. When financial authorities and conventional banking institutions tighten Anti-Money Laundering (AML) frameworks through rigid Customer Due Diligence (CDD) instruments, illicit fund flows adaptively mutate to seek the path of least resistance. The massive migration from the pure banking system toward capital markets, non-profit entities, and virtual asset ecosystems demonstrates that money laundering schemes no longer operate linearly. Levi emphasized that there is a core contradiction between general economic policy pushed hard multilaterally for liberalization of financial flows and a crime control policy intent on hampering them (Rani et al., 2024). This condition disrupts the classical financial criminal law doctrine that has hitherto overly concentrated surveillance on depository institutions, thereby demanding a new paradigm in formulating regulations capable of reaching the shadow banking ecosystem and decentralized financial instruments. Simser (2012) found that the challenges and risks posed by money laundering to financial systems and to the rule of law persist, and that understanding evolving and emerging typologies and techniques is necessary to address money laundering challenges (Bintoro et al., 2020).

Furthermore, the shift in modi operandi toward TBML and the exploitation of money mules presents extremely onerous material evidentiary complications for law enforcement. In TBML cases, criminal actors intermingle illicit fund flows with legitimate global trade traffic. The boundary between rational commercial transactions and invoice price manipulation (over-invoicing/under-invoicing) becomes exceedingly blurred, such that proving the element of

criminal intent (*mens rea*) and tracing the proceeds of crime (*follow the money*) requires forensic expertise far exceeding conventional financial auditing (Irwin et al., 2012; Patel et al., 2023a). On the other hand, the money mule phenomenon gives rise to a sociological dilemma in criminal law enforcement. The use of economically vulnerable groups as a "protective layer" in the layering instrument demands that authorities avoid being trapped in simplistic criminal liability attribution to the name appearing on the account, but rather must be capable of piercing the corporate veil or agency schemes to ensnare the intellectual actor (beneficial owner) behind them (Sultan & Mohamed, 2024).

This phenomenon of typological mutation ultimately affirms that the legal architecture of the anti-money laundering regime can no longer be operated within a reactive and siloed framework. The complexity of the intermingling of predicate offenses—such as corruption intersecting with tax evasion or terrorism financing—necessitates a shift from an administrative compliance-based approach to a risk-based approach underpinned by predictive intelligence technology. The banking and financial industries ought to be prepared for the future and continue to adapt to new emerging threats, varying consumer classifications, and changing environments, and that it is essential for compliance leaders to implement public education initiatives and help their customers recognize their role in combating money laundering and modern financing activities (Patel et al., 2023a; Tripathi & Tripathi, 2023). The effectiveness of prevention is no longer the exclusive burden of banking institutions but requires data interoperability and cross-border collaboration among monetary authorities, capital market supervisory bodies, cyber agencies, and law enforcement to mitigate exploitation gaps across various economic sectors (Bintoro et al., 2020; Menz, 2019; Tripathi & Tripathi, 2023). Levi & Reuter (2006) proposed a five-part classification of predicate offenses—drug distribution, other blue-collar crimes, white-collar crimes, bribery and corruption, and terrorism—to help understand the impact of particular money laundering controls. This classification underscores the heterogeneity of money laundering from different criminal activities and the need for differentiated regulatory responses (Akram et al., 2023).

The Constellation of Banking Crime: Fraud, Cyber Threats, and Transnational Crime

Fraud in the banking sector possesses an extremely diverse spectrum, ranging from bank loan fraud that triggers systemic losses (Naheem, 2018), credit card fraud (Koval, 2022), to sophisticated cyber schemes that sever audit trails (Simser, 2012). Alba (2000) noted that fraudulent bank loan bankruptcy is the most damaging financial crime in the Latin American region, as well as in other parts of the world, in terms of savings losses and the high social costs of bank recovery. Principles related to lending to owners and economic groups associated with the bank would be highly useful in preventing fraudulent loan bankruptcy (Naheem, 2018). Williams (2007) discussed credit card fraud as a relatively new phenomenon in Trinidad and Tobago, describing credit card typologies and the law governing such fraud, finding that the law regarding credit cards is in a very confused and unsatisfactory state (Koval, 2022). In the European Union, the most important crimes in terms of trends and typologies of the money laundering phenomenon are fraud in its various forms, including carousel fraud, social benefit fraud, investment fraud, online fraud, social engineering fraud, virtual currency fraud, and fiscal fraud (Simser, 2012). These predicate fraud offenses frequently occupy the position of a "predicate offense" that triggers a more massive chain of money laundering (Patel et al., 2023a; Tripathi & Tripathi, 2023). Patel et al. (2023a) explained that a financial fraud offense is a crime that constitutes an element of a larger crime that produces monetary proceeds; for example, generating illicit proceeds is the primary offense, and money laundering is the financial fraud offense.

On the internal side, white-collar crime presents a unique paradox for banking institutions. Shonhadji, through an analysis of agency theory and GONE theory, found that the

majority of bank employees involved in fraud are motivated by economic pressure, lifestyle demands, or hierarchical pressure from superiors. The typology of perpetrators is first viewed from the bank employee's social status, whether it comes from an honorable position or not, with honorary status referring to a high position held by the bank employee. The motives of bank employees committing fraud or white-collar crime include money, personal need satisfaction, pressure from superiors, and a non-conducive work atmosphere (Levi, 2015). The weak perception of crime exposure, combined with the perpetrator's cost-benefit analysis—where the benefits of crime are perceived as far higher than the threat of punishment—further drives the escalation of internal crime among elites (Cotoc et al., 2021). Yasir et al. (2022) found that elite-class people commit crimes upon perceiving high benefits and less punishment, and that the social environment contributes greatly to inducing criminal behavior (Cotoc et al., 2021).

The escalation of these fraud crimes is further complicated by the digital transition of banking, which brings asymmetric risks. Cybercrime, encompassing phishing, social engineering, identity theft, and point-of-sale manipulation, has a directly destructive impact on financial stability and customer trust (Alba, 2000; Williams, 2007). Akinbowale et al. (2020) found that the focus of most existing research regarding cybercrime is on the financial perspective of the banking sector and customer perception toward banking services, indicating that cybercrime has significant implications for customer perception and financial services. Tripathi & Tripathi (2023) noted that cybercrimes are a widespread annoyance and have a negative impact on society in many ways, encompassing credit card fraud, bank account fraud, point-of-sale fraud, currency fraud, identity theft, and social engineering in the banking context (Williams, 2007). Amid this digital transformation, a new and deeply concerning phenomenon has emerged: *Transaction Laundering*. This scheme is a form of violation in which perpetrators abuse legitimate digital payment merchants to process and disguise transactions that actually originate from illegal business entities (Yasir et al., 2022). Saxena (2024) argued that transaction laundering has become an increasingly intricate and rampant form of financial misconduct in the age of digital commerce, and advocated for a shift in risk management strategies, arguing that entities under obligation should harness advanced technological methods to counter transaction laundering challenges effectively.

Furthermore, the banking crime ecosystem also intersects closely with the dimension of structural and transnational crime, particularly corruption and terrorism financing. Corruption and bribery—especially involving Politically Exposed Persons (PEPs)—constitute the predicate offenses contributing the largest volume of illicit funds in many developing countries (Gavrilko, 2020). Sultan & Mohamed (2024) found that politically exposed persons are involved in most of the laundering cases in Pakistan. At the opposite pole, terrorism financing crime exhibits an anomalous pattern; its fund volumes are often smaller compared to conventional money laundering practices (Shonhadji, 2020), yet its operational techniques are far more complex because they highly prioritize a high degree of anonymity, such as through the camouflage of non-profit donation abuse and the exploitation of virtual asset instruments (Tripathi & Tripathi, 2023). Irwin et al. (2012) found that although terrorism financers use similar channels to money launderers, they do not utilize as many of the placement, layering, and integration techniques; rather, they prefer to use a few techniques which maintain high levels of anonymity and appear innocuous. The sums of money involved vary significantly; for example, the average maximum sum involved in money laundering cases was AUD 68.5 million, compared to AUD 4.8 million for terrorism financing cases (Shonhadji, 2020).

Based on the exposition of the constellation of crimes above, the phenomenon of internal white-collar crime in the banking sector represents a structural failure in corporate governance. Based on the construction of agency theory and the rational calculus of perpetrators, weak internal oversight creates an ecosystem environment in which fraud can be normalized (Levi,

2015). Shonhadji (2020) found weaknesses and errors in the practice of agency theory in banking service businesses that cause bank employees to commit fraud and white-collar crime; if the goals and performance motivation of bank employees are money-oriented, the opportunity to commit fraud or white-collar crime will persist. Fraud and white-collar crime can occur if the perception of crime exposure is low (Levi, 2015). The handling of elite bank personnel often culminates in internal settlement or mere administrative sanctions to avoid reputational panic, which in turn degrades the deterrence effect. To unravel this paradox, a reorientation of law enforcement is required that not only targets individuals in a piecemeal fashion but also optimizes the application of the doctrine of corporate criminal liability. This is crucial to compel banking institutions to build a substantive fraud prevention architecture, not merely paper compliance.

On the external dimension, the transition to digital banking creates an asymmetric vulnerability landscape, where cybercrime innovation exploits the blind spots of financial service innovation. Gavrilko (2020) analyzed that fraudulent actions in the banking sector are characterized by both external and internal natures, and that the typology of fraud in the banking sector is based on the application of various fraud classification criteria. The tendencies of external fraud with the use of cyberspace in the conditions of the coronavirus pandemic have been analyzed, and the classification of frauds in relation to customers and employees of banking institutions and ways to prevent them have been proposed (Akinbowale et al., 2020). The emergence of Transaction Laundering is tangible proof that the point of compromise has now shifted from the core banking system to third-party entities at the periphery of the ecosystem, such as payment gateways and merchant aggregators (Yasir et al., 2022). The exploitation of legitimate merchant ecosystems effectively obscures traditional audit trails. As a response, the banking mitigation framework can no longer rely solely on static Customer Due Diligence (CDD) at the point of account onboarding. A paradigm shift toward Know Your Customer's Customer (KYCC) or Merchant Due Diligence (MDD) is required, integrated with continuous transaction monitoring based on artificial intelligence to detect data traffic anomalies indicative of transaction laundering (Patel et al., 2023a; Yasir et al., 2022).

The complexity of analysis reaches its apex when banking infrastructure intersects with structurally and transnationally dimensioned crime, which in practice demands two mutually opposing investigative approaches. In corruption cases involving PEPs, banks often unwittingly transform into the primary vehicle for concealing the proceeds of corruption offenses. Law enforcement and asset recovery efforts are frequently obstructed by layered account structures concealed behind the names of PEP-affiliated family members or business entities (Gavrilko, 2020). This demands the application of aggressive Enhanced Due Diligence (EDD) and beneficial ownership transparency. Akram et al. (2023) advocated the need for much-needed empirical research between money laundering/terrorism financing and the stock market, keeping in view the growing criminal cases in developing countries, and emphasized the significance of FATF recommendations on money laundering and terrorism financing, especially for countries listed as "grey" (Saxena, 2024). At the opposite pole, the anomaly of terrorism financing that exploits very small nominal amounts (micro-structuring) through the camouflage of non-profit institutions succeeds in undermining the effectiveness of surveillance that relies solely on threshold-based monitoring (Shonhadji, 2020; Tripathi & Tripathi, 2023). Cotoc et al. (2021) found an increasing tendency toward information exchange between European Union countries regarding the suspicion of money laundering, but there is no stable trend for referring cases to law enforcement and other responsible institutions (Simser, 2012). This constellation affirms that the modern anti-money laundering architecture must operate elastically; it is required to possess high sensitivity to mitigate the macro corruption fund flows of elites, while simultaneously possessing analytical acuity to detect micro fund movements

from terrorist cells hiding behind social donation transactions (Shonhadji, 2020; Simser, 2012; Tripathi & Tripathi, 2023).

Comprehensive Classification and Mitigation Framework

Based on the data synthesis, banking crimes can be comprehensively classified into four main dimensions: the nature of the operation, which encompasses risks posed by both internal and external actors; money laundering methods, which involve banking institutions, non-bank entities, and virtual instruments; the types of predicate crimes such as drug trafficking, corruption, and terrorist financing, as well as the technological dimension exploited by perpetrators (Gavrilko, 2020; Koval, 2022; Levi & Reuter, 2006). In response to this classification, the current regulatory and mitigation frameworks, although guided by the strict standards of the Financial Action Task Force (FATF), in fact still leave structural gaps (Akram et al., 2023; Patel et al., 2023b). There are four main challenges in prevention efforts: the evolution of criminal typologies, which moves far faster than regulatory responses; knowledge gaps among law enforcement officials regarding the complexity of banking and capital market business processes (Bintoro et al., 2020); the reluctance of banking institutions to report losses from fraud to preserve reputational stability (Alba, 2000), and the varying levels of obligation regarding the adoption of advanced data mining and analytics technologies among banking entities (Saxena, 2024).

Analysis of these four-dimensional classifications indicates that contemporary banking crime no longer operates linearly but through the convergence of various elements that transcend traditional jurisdictional boundaries. The convergence of virtual money laundering methods and high-level encryption technology directly exacerbates the first challenge: regulatory lag. Positive law is often reactive and shaped by past events, while criminal innovation operates in an anticipatory and borderless manner. Consequently, soft law instruments from international organizations such as the FATF frequently encounter obstacles when transplanted into rigid national criminal legal frameworks. This leaves a legal vacuum that is quickly exploited by organized crime groups to shift their operational assets from the strictly regulated formal banking sector toward the shadow banking ecosystem or cryptocurrency.

In the realm of law enforcement, the gap in law enforcement capacity and the banking industry's defensive stance create a significant law enforcement paradox. Limited financial literacy among investigators and prosecutors—particularly regarding capital market derivatives or complex financial engineering—often causes cases to stall at the stage of proving the material elements of a criminal offense (mens rea and actus reus). This situation is exacerbated by the high rate of unreported crimes (dark number), where financial institutions often choose to resolve fraud cases—especially internal white-collar crimes—through informal restorative justice to avoid customer panic (bank runs) and a plunge in stock prices. This institutional reluctance essentially undermines the principle of transparency and hinders financial intelligence agencies (such as the PPATK) from mapping comprehensive crime typologies, thereby allowing the same criminal methods to mutate and recur in other institutions.

Faced with this asymmetry of threats and structural challenges, the mitigation framework can no longer rely solely on conventional criminal law approaches that are reactive in nature. Disparities in the adoption of data mining and artificial intelligence analytics technologies among banks create a weakest link in the national financial system, where criminal syndicates will rationally target banking institutions with the most primitive compliance infrastructure. Therefore, institutional redesign is required, whereby supervisory authorities, such as the Financial Services Authority (OJK), mandate minimum standards for regulatory technology (RegTech) and supervisory technology (SupTech) for all reporting entities. Harmonizing

efforts to improve financial forensic literacy among law enforcement, eliminating the culture of absolute bank secrecy that shields perpetrators, and implementing reporting obligations based on algorithmic detection will transform the mitigation framework from mere administrative compliance (tick-box compliance) into a robust and proactive multi-layered defense ecosystem

CONCLUSION

The landscape of banking crime has evolved into a complex, asymmetric, and highly adaptive ecosystem. Contemporary banking crime is no longer dominated by conventional physical robberies but has evolved into money laundering using hybrid techniques (such as structuring, Trade-Based Money Laundering, and the use of money mules), internal and external cyber fraud, terrorist financing, and corruption by institutional elites. This reality underscores the existence of "regulatory arbitrage" that systematically exploits the gap between financial technology innovation and the lag in positive law.

Facing these ever-evolving threats, the banking industry and law enforcement agencies can no longer rely solely on administrative compliance procedures or traditional Customer Due Diligence (CDD). Holistic and progressive policy reforms are required, encompassing the integration of artificial intelligence-based risk mitigation technologies (RegTech and SupTech), the strengthening of the doctrine of corporate criminal liability, and the enhancement of legal information-sharing cooperation instruments across jurisdictions. A comprehensive understanding of the typology of these crimes is a fundamental prerequisite, not only for formulating responsive laws, but also for securing the stability of the national and global financial architecture in the future.

REFERENCE

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, *27*(3), 945–958. https://doi.org/https://doi.org/10.1108/JFC-03-2020-0037

Akram, T., Ramakrishnan, S. A., & Naveed, M. (2023). Prevalence of money laundering and terrorism financing through stock market: a comprehensive conceptual review paper. *Journal of Money Laundering Control*, *26*(5), 1027–1044. https://doi.org/10.1108/JMLC-06-2022-0094

Alba, R. M. (2000). Fraud control in offshore banking centres. *Journal of Money Laundering Control*, *3*(3), 245–249. https://doi.org/https://doi.org/10.1108/eb027236

Bintoro, S., Sjamsuddin, S., Pratiwi, R. N., & Hermawan. (2020). International cooperation to combat money laundering in the capital market: Indonesia and Australia experience. *Journal of Investment Compliance*, *21*(4), 263–276. https://doi.org/https://doi.org/10.1108/JOIC-10-2020-0043

Cotoc, C.-N., Nițu, M., Șcheau, M. C., & Cozma, A.-C. (2021). Efficiency of money laundering countermeasures: case studies from European Union member states. *Risks*, *9*(6), 120. https://doi.org/10.3390/risks9060120

Gavrilko, T. O. (2020). Risks of fraud in the field of financial services. *Publishing House "Baltija Publishing."* https://doi.org/10.30525/978-9934-588-61-7-4

Ibraj, B. (2016). Money Laundering in Albania for the Years 2008-2015. *European Journal of Economics and Business Studies*, *2*(3), 101–110. https://doi.org/10.26417/ejes.v6i1.p101-110

Irwin, A. S. M., Choo, K. R., & Liu, L. (2012). An analysis of money laundering and terrorism financing typologies. *Journal of Money Laundering Control*, *15*(1), 85–111. https://doi.org/10.1108/13685201211194745

Koval, Y. (2022). Comparative Analysis of Methods for Counteracting the Legalization (Laundering) of Income Obtained by Criminal Means. *The Economics of Uncertainty: Content, Evaluation and Regulation*, 113.

Levi, M. (2015). Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research*, *21*(2), 275–297. https://doi.org/https://doi.org/10.1007/s10610-015-9269-7

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice*, *34*(1), 289–375.

Menz, M. (2019). Beyond placement, layering and integration–the perception of trade-based money laundering risk in UK financial services. *Journal of Money Laundering Control*, *22*(4), 614–625. https://doi.org/10.1108/JMLC-12-2018-0070

Naheem, M. A. (2018). China's dirty laundry–international organizations posing a risk to China's AML systems. *Journal of Money Laundering Control*, *21*(2), 189–202. https://doi.org/https://doi.org/10.1108/JMLC-08-2015-0032

Patel, S., Kasztelnik, K., & Zelihic, M. (2023a). *Global overview of modern financing typologies to mitigate financial risks in development countries*. https://doi.org/10.21272/sec.7(2).54-66.2023

Patel, S., Kasztelnik, K., & Zelihic, M. (2023b). The observational study financial fraud offense themes and financial fraud risk of money laundering to increase financial global sustainability compliance. *Journal of Accounting & Finance*, *23*(4), 1–19. https://doi.org/10.33423/jaf.v23i4.6446

Rani, M. I. A., Nazri, S. N. F. S. M., & Zolkaflil, S. (2024). A systematic literature review of money mule: its roles, recruitment and awareness. *Journal of Financial Crime*, *31*(2), 347–361. https://doi.org/https://doi.org/10.1108/JFC-10-2022-0243

Saxena, C. (2024). Identifying transaction laundering red flags and strategies for risk mitigation. *Journal of Money Laundering Control*, *27*(6), 1063–1077. https://doi.org/https://doi.org/10.1108/JMLC-11-2023-0182

Shonhadji, N. (2020). Paradox of white collar crime and fraud in banking: Critical analysis of agency theory and gone theory. *Assets: Jurnal Akuntansi Dan Pendidikan*, *9*(2), 142–155.

Simser, J. (2012). Money laundering: emerging threats and trends. *Journal of Money Laundering Control*, *16*(1), 41–54. https://doi.org/https://doi.org/10.1108/13685201311286841

Sultan, N., & Mohamed, N. (2024). The money laundering typologies and the applicability of placement-layering-integration model in undocumented South Asian economies: a case of Pakistan. *Journal of Money Laundering Control*, *27*(4), 741–762. https://doi.org/https://doi.org/10.1108/JMLC-08-2022-0116

Tiwari, M., Ferrill, J., & Allan, D. M. C. (2025). Trade-based money laundering: a systematic literature review. *Journal of Accounting Literature*, *47*(5), 1–26. https://doi.org/https://doi.org/10.1108/JAL-11-2022-0111

Tripathi, R., & Tripathi, S. (2023). Identifying Fraud Detection Techniques Using Text Analytics Processing. *Adhyayan: A Journal of Management Sciences*, *13*(01), 5–8. https://doi.org/https://doi.org/10.21567/adhyayan.v13i1.02

Williams, D. A. (2007). Credit card fraud in Trinidad and Tobago. *Journal of Financial Crime*, *14*(3), 340–359. https://doi.org/https://doi.org/10.1108/13590790710758521

Yasir, A., Ahmed, A., & Anum, L. (2022). Corporate financial crimes in Pakistan–a review and analysis. *Journal of Financial Crime*, *29*(3), 1064–1077. https://doi.org/10.1108/JFC-10-2021-0233