FROM RISK TO RESILIENCE: STRENGTHENING AML FRAMEWORKS IN BANKS AMID EMERGING LAUNDERING TECHNIQUES

By

ZMARIALY YOUSUFI *   **HARIKUMAR P. N. ****

Institute of Management in Kerala (IMK), University of Kerala, Thiruvananthapuram, Kerala, India.
Department of Commerce, University of Kerala, Thiruvananthapuram, Kerala, India.

ABSTRACT

Money laundering remains a global threat that undermines financial stability and erodes trust in banking systems. Banks are particularly vulnerable given their broad customer base, diverse products and services, and technology-driven operations, which expose them to reputational, operational, and legal risks. This paper synthesizes secondary data and regulatory sources to examine the money laundering risks and challenges banks face, with specific attention to technological dimensions. Building on international standards such as FATF recommendations, Basel Principles, and the EU AMLD, the study proposes a Risk-to-Resilience AML Framework that integrates core compliance measures, such as the Risk Based Approach, Customer Due Diligence, Suspicious Transaction Reporting, and Beneficial Ownership transparency, with technology adoption as a moderating factor. The findings suggest that while money laundering risks cannot be fully eliminated, banks can strengthen resilience through risk-based programs, technological innovation, and adherence to global AML standards. By linking compliance effectiveness to organizational resilience, this study contributes a novel conceptual perspective that informs both policy and practice in the evolving fight against financial crime.

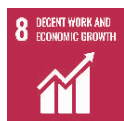*Keywords: Anti Money, Banks, FATF, Anti-Money Laundering Risk.*

INTRODUCTION

The term "money laundering" has been defined in different ways by different researchers: "The conversion or transfer of property, knowing that such property is derived from serious crime, to conceal or disguise the illicit origin of the property or of assisting any person who is involved in committing such an offense or offenses to evade the legal consequences of his action and the concealment or disguise of the true nature, source, location, disposition, movement, rights concerning, or ownership of property, knowing that such property is derived from serious crime"

This paper has objectives related to SDG

(Bhure, L. 2003). The Palermo convention definition for money laundering is "the conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his actions." Money laundering depends on deceit: its purpose is to conceal the true source, ownership, and use of illegally obtained funds and to make them appear legitimate. Globally, laundering is substantial-analysts estimate it accounts for roughly 2–5% of world GDP annually (about $800 billion to $2 trillion). Money laundering enables criminals to obscure the true origin of illicit funds and present them as proceeds from legitimate activities. By routing those proceeds through concealed channels, perpetrators can place assets beyond the reach of forfeiture laws and regulatory scrutiny. Money

laundering disguises the source of criminal activity's proceeds to incorporate them into the legitimate financial community. Sullivan, K. (2023) defined money laundering as the process of making illegally obtained funds appear legitimate, even though they originated from unlawful sources. The process typically involved three stages: placement, where illicit funds were introduced into the financial system; layering, which included complex transactions to obscure their origin; and integration, where the funds re-entered the economy as seemingly legitimate money (Madinger, 2011).

The Financial Action Task Force (FATF) is in charge of promoting anti-money laundering (AML) recommendations to international governmental organizations. A key element of the FATF's efforts is its comprehensive set of standards, which member countries can adopt and implement. Additionally, the FATF has released a number of interpretive notes to offer further information and make clear how particular suggestions should be put into practice. The FATF's guidelines have served as the foundation for the development of an effective national and international AML and CFT-related control approach. The FATF Recommendations are accepted by the World Bank and IMF as the international norms for preventing money laundering and the funding of terrorism (FATF, 2012–2025). The FATF 40 Recommendations cover a comprehensive range of preventive measures against the funding of terrorism and money laundering. These include financial system regulation and recognition of money laundering risk, the criminal justice system and law enforcement, transparency of legal entities and agreements, and international cooperation.

Typically, money laundering involves several different transactions to hide the reliable source of financial assets, permit the use of the proceeds, and protect the offenders. Money laundering acted as a critical tool for various groups, including organized crime syndicates, terrorists, drug traffickers, and insider traders, seeking to avoid scrutiny from authorities that sudden profits from illegal activities would attract (Sullivan, K. 2023). To avoid detection by law enforcement, drug traffickers and other criminal organizations have developed several highly sophisticated strategies and tactics. These include multiple advantageous entry points into the global financial system, prompt and insufficient oversight of the transfer of large amounts of money through banks and other financial operations, the attraction of corruption and bribery in the murky world of finance, and the existence of unofficial, parallel economies that are not subject to state regulation (Bhure, L. 2003). There is a need for coordinated international action against these persistent threats, which have an impact on everything from large outflows of trillions of dollars due to organized crime and corruption to well-funded terrorist actions. The threats of international money laundering and terrorist financing are still growing (Basel, 2023). Given the significance and gravity of the issue, this paper explores the risks and challenges that money laundering poses to banks, and examines strategies banks can employ to mitigate and manage these risks (Basel, 2023).

1. Objective

This study investigates the potential risks of money laundering in banks and examines international initiatives and measures designed to combat it. In particular, it focuses on anti-money laundering strategies, preventive practices, and the development of robust programs to safeguard banks against money laundering activities.

2. Literature Review

Examined the banking sector's efforts to fight against money laundering and how the phenomenon plays out in the day-to-day activities of Finnish bank employees (Juntunen & Teittinen, 2023). The study aimed to demonstrate responsibility and the bank's function in Finland's fight against money laundering. According to survey findings, understanding customer is one of the greatest crucial elements in combating money laundering. Risk-based anti-money laundering strategies, customer risk classification, and internal banking policies have all contributed to clarifying routine AML procedures. Advancements in technology and the proliferation of payment services have introduced new methods of money laundering. At the same time, technology has

aided in monitoring cash flows through various software and surveillance systems. A key challenge, however, is that regulations governing customer behavior in different scenarios are constantly evolving. A study based on Malaysian banks was conducted to investigate the relationships between customer knowledge of money laundering and terrorism financing, belief in banking secrecy measures, discomfort with the bank's anti-money laundering (AML) procedure, and acceptance of the bank's current counterterrorism financing and AML practices (Azman Aziz & Md Daud, 2022). The study revealed a substantial correlation among the respondents' awareness of money laundering and financing of terrorism, their confidence in banking secrecy measures, and their reception of the bank's anti-money laundering and counter-terrorist financing activities. However, there is no conclusive evidence between the degree of pain clients feel in meeting the bank's AML criteria and their acceptance of its AML operations. Even after adjusting for potential reasons for the customer's approval of banking practices considered in the existing literature, such as age, gender, geography, reading level, and occupation, these findings remain valid.

The study aimed to determine how banking officers saw the factors influencing anti-money laundering compliance and money laundering mitigation (Zakaria et al., 2022). Regulatory thoroughness, training, and awareness were the three independent variables used in the study to evaluate and assess the level of perceived compliance among the banking compliance officers. The information was gathered by sending questionnaires to 56 Malaysian banks. According to the study's findings, the perceived level of compliance was positively correlated with regulatory comprehensiveness, training, and awareness. The report suggested that banking institutions should strengthen anti-money laundering regulations and policies to increase the effectiveness of Malaysia's financial institutions. The compliance officer's expertise must also be improved to ensure higher compliance quality.

The study aimed to evaluate Pakistan's anti-money laundering & countering the funding of terrorism (AML/CFT) policies and their effects on the risk of money laundering (Jaffery & Mughal, 2020). The research used vital variables to examine the effects of customer due diligence, wire transfers, record keeping, correspondent banking, new technology, reporting of transactions, compliance, internal controls, training, and AML/CFT rules in Pakistan. Data was gathered using questionnaires that were created in accordance with the Financial Actions Task Force's (FATF's) recommendations and Pakistan's AML/CFT rules. One hundred two workers who worked in the compliance departments of several banks in Pakistan provided information for the study. According to the study's conclusions, customer due diligence, correspondent banking, and new technology may all aid in reducing Pakistan's risk of money laundering. The risk of money laundering was unaffected by the influence of record keeping, wire transfers, or transaction reporting. The report recommends a better application of these actions. The report includes recommendations for enhancing the management and mitigation of money-laundering risk in Pakistan and insights into the efficacy of AML/CFT procedures in that nation.

The study aimed to examine the EU's (European Union) de-risking incentives and suggest model solutions to temper the idea (Rose, 2020). By examining current regulatory and economic situations, the study used a functional approach to law and economics to increase the effectiveness of fighting money laundering. The analysis discovered that the EU's de-risking policy contradicts the current regulatory framework's anti-money laundering objectives. It recommends dividing the analysis of de-risking into national and regional/union levels. A proactive strategy of contracting the client base is advised to prevent pointless regulation at the national level. The report recommends strengthening control, financial oversight, and sanctions at the regional level to build inclusion and confidence. The study clarified the importance of adopting a proactive contracting strategy to reduce de-risking and prevent financial exclusion. It makes the case that institutions should negotiate with customers at the federal level to reduce societal costs. At

the regional level, institutions may face higher transaction costs than the social cost of inclusion, necessitating tighter oversight and management. In conclusion, the study offered perceptions into the de-risking problem in the EU and suggested a proactive strategy of re-contracting the client base to combat money laundering successfully.

The goal of the study was to create a potential technique of MLTF risk assessment in non-bank businesses that are covered by Australia's AMLCTF Tranche II anti-money laundering and counterterrorism financing regulations by recommending a scorecard of risk assessment under its many dimensions, and based on the literature on credit scoring models, the objectives are met (Sathye & Islam, 2011). An analogy-based approach was employed to create a risk assessment model for the AMLCTF II, and the components of a standard credit-scoring model were modified appropriately. Theories of money laundering regulation serve as the theoretical foundation for this essay. According to theory, there is an inverse relationship between the amount of money laundering and the regulations governing it. The cost of money laundering increases with the effectiveness of the regulatory system, which results in less money laundering overall. It was discovered that the AMLCTF Tranche II would subject organizations like accounting firms to several requirements. These requirements call for detecting, reducing, and managing ML TF risk from delivering goods or services. Entities must handle two risks: business risk (including inherent and residual risks) and regulatory risk. After defining MLTF risk, the next challenge is figuring out how to recognize and rate it. The reporting entity must consider the following three things: Determine risk mitigation and control measures according to the amount of risk detected by evaluating the possibility and impact of the risk, its level, and its impact.

A review of the existing literature revealed that most studies primarily focused on broad themes such as the Financial Action Task Force (FATF), anti-money laundering (AML) compliance, the effectiveness of AML laws and regulations, and risk-based AML approaches. Sub-themes included cryptocurrency and money laundering, customer due diligence, beneficial ownership and PEPs, and terrorist financing. Very few studies, however, specifically addressed money laundering risks and challenges in the banking sector or explored robust programs to mitigate money laundering in banks. Hence, this study attempt to discuss the money laundering risks, and preventative measures/ program to prevent money laundering in banks.

3. Methodology

The study is qualitative and employs a descriptive research design, which facilitates the exploration of money laundering risks faced by banks and the corresponding preventive measures. In this study, the main ML risk to the bank and essential elements of an effective AML program to mitigate those risks in the banking sector have been investigated through document review. Data for this study was collected from secondary data sources. These secondary sources relevant to the scope of money laundering typology assessment, money laundering risk assessment by international AML organizations, and the international anti-money laundering standards and recommendations to fight against money laundering have been investigated through document review and qualitative narration to achieve the study's objectives. As the study is purely relay on secondary data and the lack of empirical validation is the limitation of the study, and the future studies could focus on empirical insights.

4. Proposed Conceptual Framework

The financial sector, particularly banks, operates under constant threat from evolving money laundering (ML) and terrorist financing (TF) techniques. Traditional compliance-based responses typically prove reactive, narrowly focused on legal adherence rather than building long-term resilience. To address this, the proposed conceptual framework is anchored in global anti-money laundering (AML) standards, primarily the Financial Action Task Force (FATF) Recommendations and supported by complementary international guidelines such as the Basel Committee on Banking Supervision (BCBS), the Wolfsberg Principles, and the European Union AML

Directives (AMLDs). This framework conceptualizes the progression from risk identification to resilience building, linking regulatory standards with organizational practices. The FATF's 40 Recommendations serve as the backbone of the framework. Rather than treating them as a checklist, this framework organizes them into five conceptual dimensions relevant to banks:

- *Risk-Based Approach (Recommendation 1):* Encourages banks to assess and mitigate risks proportionately, shifting AML from rigid rule-following to adaptive, risk-sensitive decision-making.

- *Customer Due Diligence (CDD) and Know Your Customer (KYC) (Recommendation 10–12):* Provides mechanisms to verify customer identity, understand beneficial ownership, and prevent misuse of accounts for illicit purposes.

- *Suspicious Transaction Reporting (STRs/SARs) (Recommendation 20):* Requires financial institutions to identify and report unusual activities, acting as the frontline defence in AML surveillance.

- *Beneficial Ownership Transparency (Recommendation 24–25):* Addresses the opacity of shell companies and complex ownership structures by mandating disclosure and registries.

- *Technology and Innovation (Recommendation 15):* Stresses the importance of adopting new technologies, including AI-driven transaction monitoring, blockchain analytics, and RegTech solutions, to stay ahead of evolving laundering techniques.

Furthermore, international standards such as the Basel Committee (BCBS) Principles reinforce risk management, corporate governance, and supervisory oversight as enablers of FATF compliance; the Wolfsberg Principles stress practical applications in correspondent banking, sanctions screening, and monitoring of cross-border transactions; and the EU AML Directives (4th–6th AMLD) provide region-specific emphasis on beneficial ownership registers, corporate liability, and the regulation of crypto-assets and virtual asset service providers (VASPs). Together, these standards provide supporting and operational depth needed to translate FATF's principles into actionable institutional practices. The framework highlights four essential compliance components: risk-based approach, customer due diligence (CDD)/know your customer (KYC), suspicious transaction reporting (STR), and beneficial ownership transparency as primary antecedents of AML compliance. These measures represent critical mechanisms through which banks mitigate risks, prevent financial misuse, and align with global standards. In addition, the framework acknowledges the increasing significance of emerging technologies, including Artificial Intelligence (AI), blockchain, and regtech solutions. These technologies are positioned as moderators that enhance the effectiveness of compliance mechanisms, enabling institutions to better anticipate and respond to evolving laundering methods. Finally, AML compliance itself is conceptualized as a driver of organizational resilience, ensuring that banks remain robust and adaptive in the face of new laundering challenges. In the context of AML, organizational resilience is interpreted as a multidimensional outcome encompassing regulatory compliance, effective risk mitigation, adaptability to evolving threats, and the preservation of stakeholder trust and legitimacy.

Figure 1 shows the Risk-to-Resilience AML Framework, which illustrates that AML resilience is not achieved solely through compliance with regulatory standards but is strengthened through a risk-based approach, robust reporting mechanisms, transparency in beneficial ownership, and the strategic adoption of advanced technologies. In this way, the framework provides both a conceptual and practical pathway for banks to transition from risk exposure to resilience in the evolving financial landscape.

5. Discussion

5.1 Money Laundering Methods

Money laundering is a dynamic process, with new methods and strategies continually emerging. International organizations and experts have identified many money laundering methods through typologies
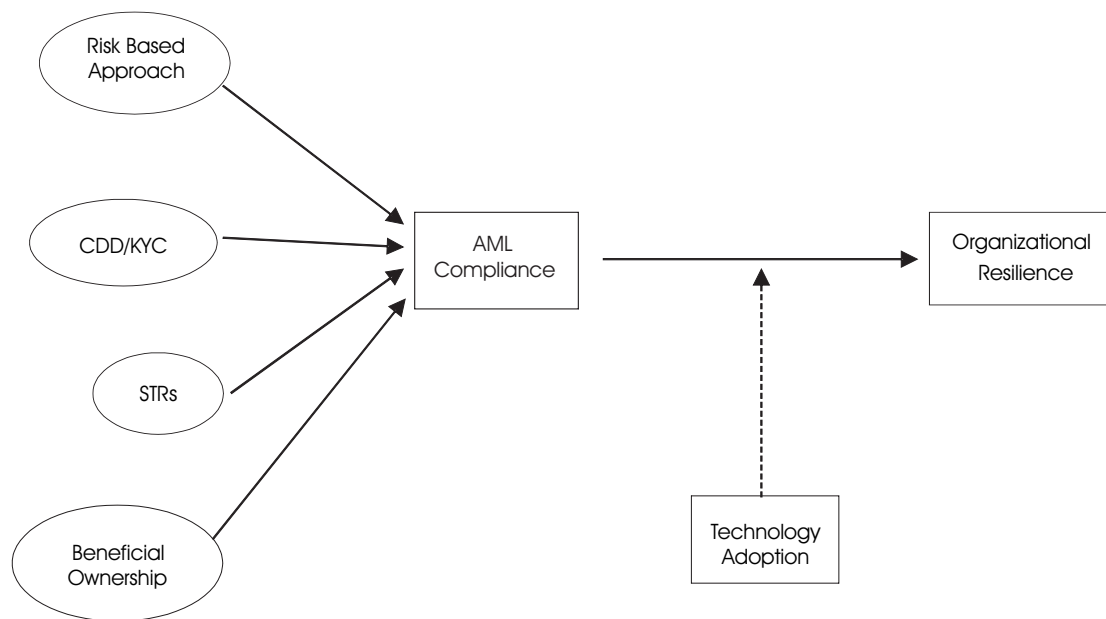
Figure 1. Risk-to-Resilience AML Framework

and cases, but many remain unidentified. Three methods are mainly used to launder money:

Moving of Money Physically (Bulk Cash & Gold Smuggling): Smuggling large amounts of cash is a popular and effective way to launder gains obtained through illegal means. The layering process began when money was taken abroad to a country with stringent bank secrecy laws. Similar to cash smuggling, large sums were concealed on a person, in luggage, or in vehicles, boats, or cargo. Another method of exporting drug proceeds involved using gold: illicit funds were used to buy gold from wholesalers or refiners, which was then melted down and fashioned into low value items such as bolts, nuts, car parts, or tools. These objects were painted silver or gray to improve concealment. The gold was then hidden and transported by courier or air cargo. The organization typically held the gold until market prices were favorable, although it could be sold at any time.

Financial System (Organized or Unorganized): Using a financial system's various products and services. Money service businesses frequently transfer money from one location to another. These businesses include Western Union, postal service-style money transmitters, stored value issuers, issuers of traveler's checks, and money

transfer agents. A money service company typically provides an extensive range of valuable services for money laundering. Two widely used methods are airline tickets and foreign exchange. The benefits of a money remitter, such as wire transfers, faxes, drafts, checks, or couriers, are specifically designed to give those unable to use standard banking institutions a way to send money. Transferring small amounts of money that foreign nationals wish to send to their families back home is legal. The most commonly used method for sending large sums across borders is bank wire transfers. Wire transfers are a key component of the layering process. Once the money has been deposited in a bank, it is shifted through a series of transactions intended to confuse law enforcement.

Trade System and Physically Moving Goods: An alternative remittance system is referred to as trade-based money laundering. The Financial Action Task Force (FATF) defines trade-based money laundering as hiding and transferring wealth through trade transactions to give legitimacy to the illegal sources of the proceeds of crime. This can be accomplished in reality by falsifying the cost, volume, or quality of imports or exports. To further disguise the money trail, trade-based money laundering strategies come in various sophisticated forms and are

typically combined with other methods. The most prominent methods of trade-based money laundering are over-invoicing, under-invoicing, and fake invoicing.

5.2 Money Laundering Risks and Challenges to Bank

The UNODC estimates that 2–5% of global GDP is laundered each year. UNODC (2011) noted that the use of banking channels to transfer illicit funds for money laundering and terrorist financing compromises the integrity of the financial system. Financial institutions, especially banks, are the preferred medium for criminals to launder illegal funds (Sundarakani & Ramasamy, 2013). This is mostly attributable to three factors: Banks first provide many services and mechanisms, such as bank drafts, cash transfers (local and international), and foreign correspondent accounts, which enable the movement of monies under the pretense of legitimacy. The global expansion of banks and technical improvements have enabled a more secure, rapid, and convenient method for international financial transfers, therefore complicating the tracking of money's sources (Viritha et al., 2015).

Banks have been significantly targeted historically and currently throughout the three phases of money laundering. Due to the wide range of products and services provided by banks and broad segments of customers and clients, it is more exciting and targeted for money laundering. Banks potentially attract money laundering because of the nature and coverage of the institution, a wide range of products and services, a variety of services to different segments of customers, and technology-driven facilities. Particular areas of interest and concern regarding using of banks for money laundering includes: electronic transfer of money, correspondent banking, politically exposed persons (PEPs), structuring/ micro structuring, cyber banking/ internet banking, smart cards, ATMs, credit cards and prepaid cards.

Money laundering presents considerable risks and obstacles to banks and financial organizations. The risks encompass legal, operational, reputational, and financial dimensions. The following outlines the principal risks and obstacles that banks encounter about money laundering:

- *Legal and Regulatory Risks:* Failure to adhere to Anti-Money Laundering (AML) laws can lead to heavy fines, sanctions, or even loss of banking licenses (Non-compliance penalties). Regulators may impose stricter oversight or audits, increasing compliance costs and operational burden (Increased scrutiny). In some jurisdictions, bank officials can face prosecution if the bank is complicit or negligent in facilitating money laundering (Criminal liability).

- *Reputational Risk:* Association with money laundering cases can damage a bank's reputation among customers and investors (Loss of public trust). High-profile cases receive negative media attention, which can affect the bank's market value and business relationships. (Media exposure).

- *Operational Challenges:* Detecting suspicious transactions among millions of legitimate ones is difficult, especially with sophisticated laundering schemes (Complex transaction monitoring). Banks must invest heavily in AML systems, staff training, and compliance departments (Resource-intensive compliance). Large volumes of customer and transaction data must be analyzed, managed, and reported accurately to regulators (Data management).

- *Financial Risks:* Involvement in laundering schemes may result in losses due to fraud, fines, and legal costs (Direct financial loss) Authorities may freeze or seize assets believed to be tied to criminal activities, impacting liquidity (Asset seizure).

- *Technological Challenges:* Criminals use new technologies, such as cryptocurrencies, to obscure money trails (Rapidly evolving techniques). Money launderers may exploit cybersecurity weaknesses to penetrate systems and move illicit funds (Cybersecurity threats).

- *Globalization and Cross-Border Complexity:* Different AML laws across countries can complicate investigations and compliance efforts (Jurisdictional

issues). Obscure ownership and origins of illegal funds (Shell companies and offshore accounts).

- *Challenges with Customer Due Diligence (CDD):* It is typically hard to identify the real owner behind legal entities or trusts (Identifying beneficial ownership). Ensuring thorough background checks during customer onboarding is essential but can delay business (Onboarding risks).

Banks play a critical role in preventing money laundering. They must balance their business goals with stringent compliance requirements. Effective AML programs, robust internal controls, and continuous staff training are essential to mitigating these risks and safeguarding the financial system. FATF continues to emphasize risk-based supervision for banks to allocate controls proportionate to risk, moving beyond tick-box compliance.

5.3 International Anti Money Laundering Initiatives

The issue of money laundering is worldwide in nature, and combating it requires international cooperation. Several initiatives have been launched to approach the issue from a global perspective. By the end of the 1980s, some steps were taken by international organizations, including the United Nations and the Bank for International Settlements, to address the issue (United Nations, 2000). Several regional establishments, including the Organization of American States, the Council of Europe, and the European Union, created anti-money laundering guidelines for their member nations. At the same time, the Financial Action Task Force (FATF) was established in 1989. Region-specific anti-money laundering task forces have been established in the Caribbean, Asia, and Eastern Europe. The leading international organizations that deal with money laundering and developing anti-money laundering standards and strategically work for a sound AML framework and AML preventative measures are:

Financial Action Task Force: The FATF was created as an intergovernmental agency with 34 member nations and two international organizations by the G-7 Summit in Paris in 1989. Its primary goal is to set standards against money laundering and the financing of terrorism. Its most significant initiative was the introduction of 40 Recommendations on Anti-Money Laundering and Terrorist Financing, representing a remarkable effort to establish a robust framework for AML and provide practical guidance for institutions, regulatory bodies, and law enforcement agencies.

FATF-Style Regional Bodies (CFATF, EAG, APG, GABAC, MONEYVAL, GIABA, GAFILAT, ESAALMG, and MENAFATF): FATF-style regional organizations with a structure and operations close to the FATF. Offer suggestions for standards and typologies to the FATF and help assess FATF members.

Basel Committee on Banking Supervision: The G10 central banks established the Basel Committee on Banking Regulations and Supervisory Practices to advance sound supervisory practices globally. Some of the critical publications about money laundering and terrorist financing include "Consolidated KYC risk management paper, customer due diligence for banks, general guide to account opening and customer identification, sharing of financial records among jurisdictions in connection with the fight against terrorist financing, and sound risk management of money laundering and terrorist financing."

The Council of Europe Convention on Laundering (European Union Directives on Money Laundering) is a 28-member political-economic union focusing on Europe. Establishes AML/CFT directives about laws that member states must enact to stop money laundering and terrorism financing from occurring through their financial systems. The Council issued several directives to prevent the use of the financial system for money laundering, including the EU First Directive in 1991, the Second Directive in 2001, the Third Directive in 2005, and the Fourth Directive in 2015.

Organization of American States: The Organization of American States commission that handles everything about drugs, including money laundering.

Egmont Group of Financial Intelligence Units: informal network of financial intelligence units (FIUs); its issued documents are "statement of purpose, best practices for the exchange of information between financial intelligence units, and principles for information

exchange between financial intelligence units for money laundering cases."

Wolfsburg Group: Association of 13 international banks to create standards for money laundering procedures for banks.

World Bank and the International Monetary Fund: The groups collaborate and operate with the FATF to support nations. To examine FATF member countries' anti-money laundering policies and legislation and ensure they are appropriate.

5.4 Anti-Money Laundering Program and Practice for Bank

Any financial institution must develop a quality AML/CFT program to prevent money laundering in the organization, report suspicious activities, and promote AML/CFT awareness to all staff within the institution. Such programs may differ from organization to organization based on size, coverage, and other factors. The four pillars of a quality AML program in a financial institution are internal policies and procedures/control, designating an authorized officer, autonomous audit function, and staff training. The AML policy and procedures of the institution should include the detailed potential risks the institution faces and a comprehensive plan to overcome those risks. The designated compliance officer is responsible for the day-to-day AML compliance functions and the smooth running of the overall AML program within the organization. An independent internal audit function must be carried out by an individual or unit in an organization to ensure the overall success of evaluating the AML program within the organization independently. To achieve successful AML program implementation within the organization, it is crucial to communicate the established pillars mentioned above to the financial institution's employees. Hence, a comprehensive training regime that covers all employees periodically must be established.

Since banks offer a wide range of products and services to a vast clientele, money laundering is more likely to occur within banking institutions. It could expose the banks to risks related to their reputation, operations, and law.

Thus, an anti-money laundering/counter-terrorist financing (AML/CFT) program is vital to a bank compliance system. Protecting the bank from financial crimes such as money laundering and financing of terrorism and ensuring the bank complies with all applicable rules and regulations are the main objectives of an AML/CFT program. Therefore, any banking institution's main priorities should be creating, organizing, and implementing these initiatives. The FATF 40 recommendations and its interpretative notes discuss the core standards for preventing and mitigating money laundering risks/threats. The recommendations specify the essential measures at the international, national, and institutional levels and require the member countries to follow and adopt the standards to build a strengthened AML regime. The core elements of an effective AML program for banks and financial institutions in the context of FATF recommendations include money laundering/terrorist financing (ML/TF) risk assessment and management, customer acceptance policy and customer due diligence (KYC/CDD/EDD), ongoing monitoring systems, suspicious transaction reporting, and record keeping. Meanwhile, the Basel Committee, with the concurrence of FATF, released sound management of risks associated with money laundering and terrorism financing in February 2016, and updated it in 2020. The norm is about managing risks of money laundering and terrorism funding and how banks should include them in their comprehensive risk management scheme. According to the guideline, careful management of these risks and adequate oversight supervision are essential to preserving the financial system's integrity and the banks' safety and soundness. Banks run significant operational, compliance, reputational, and other risks if these risks are not managed. The guideline stresses the following major requirements for a bank to mitigate the money laundering risk:

- *Risk Analysis and Governance:* Identifying and analyzing the risks is the first stage in controlling money laundering (ML) issues. This will help with the design and successful implementation of suitable measures. Among other levels, the analysis should

cover relevant inherent and residual risks at the national, sector, bank, and business relationship levels. Risk assessments should be recorded and made available to supervisors and other authorities. This assessment facilitates meetings with other bank stakeholders to identify potential risks and develop appropriate countermeasures. Appropriate governance mechanisms, which establish a compliance culture with a strong tone from the top, are another crucial component. As the bank's senior management, the board of directors has crucial oversight responsibility. They should approve and oversee all risk, compliance, and risk management policies. To make informed decisions, the board must have a thorough understanding of money laundering (ML) risks, supported by timely, accurate, and comprehensive risk assessment information. Along with senior. This senior-level officer should be granted sufficient authority to ensure that when concerns arise, the board, senior management, and business units take appropriate action. The board should also provide the AML officer with the necessary resources to effectively oversee the day-to-day implementation and success of the bank's AML activities, as this officer acts as the board's representative in ensuring adherence to the bank's AML program.

- *Three Lines of Defense:* The Committee outlines the bank's three lines of defense for its anti-money laundering (AML) efforts. The line of business serves as the first line of defense, responsible for developing, implementing, and maintaining AML-related policies and procedures. It ensures that all employees are informed about these policies and establishes guidelines for employee screening to uphold the highest standards of ethics and professionalism. Furthermore, it provides appropriate AML training tailored to employees' roles and functions, ensuring they clearly understand their responsibilities. The second line of defense is the AML compliance function, which includes the human resources, technology, and broader compliance departments.

The AML Officer oversees continuous monitoring of AML compliance across all operations, ensuring that any identified instances of non-compliance or irregularities are promptly escalated to senior management and, when necessary, to the board. This monitoring process involves activities such as sample testing, exception report reviews, and overall compliance assessments to maintain adherence to regulatory and internal AML requirements. The AML Officer should be independent of the business lines, be the point of contact for all AML matters for internal and external authorities, and report suspicious transactions. Internal audits as a third line of defense must independently assess the bank's risk management and controls regularly, reporting to the board of directors' audit committee (or a comparable oversight body). These assessments should cover the following topics: how well the bank's staff executes the controls, how well the compliance oversight and quality controls work, and how adequate the bank's controls are in mitigating the identified risks. Competent staff members with adequate audit experience in the audit function are required. A bank-wide audit should be carried out regularly, with the frequency of audits determined by risk. To assess the program's efficacy, audits must be appropriately scoped, including the employment of outside auditors. Auditors should pursue their findings and recommendations proactively.

- *Customer Acceptance and Due Diligence:* Banks should also create a Customer Acceptance Policy to identify customers likely to pose a higher risk of money laundering and relationships that the bank will not accept. For every consumer, banks should perform a baseline level of due diligence; when risks rise, they should intensify that effort. Specific clients might qualify for streamlined due diligence when there is little chance of money laundering, depending on the relevant regulations. Banks should handle risk profiling, identification, and verification of customers and beneficial owners in their CDD policies. Banks must verify the identities of both beneficial owners

and clients as part of this process. Banks should interact with customers or complete transactions only after the customer's identity has been verified (unless doing so would disrupt normal business operations, in which case appropriate controls should be implemented while CDD and verification are being conducted). Identity verification needs to be done using trustworthy methods. Banks may utilize a written statement from the customer to determine beneficial ownership, but they should rely on something else. The bank should not open an account or close any opened accounts. If CDD cannot be completed or the customer's identity cannot be verified, the bank should consider reporting such behavior as suspicious to the relevant authorities. This also applies to anonymous accounts.

- *Ongoing Monitoring and Transaction Monitoring Systems:* AML concerns necessitate more than just suitable policies and processes; banks also need adequate and appropriate monitoring systems, as the transactional monitoring system is essential to minimizing ML risk within the bank. Typically, banks will use an IT monitoring system in this situation. The bank should provide documentation explaining its rationale for not considering an IT monitoring system necessary. Every account and transaction made by a bank customer should be monitored, allowing for the study of activity trends and the discovery of odd business connections and transactions, especially when it comes to alterations in the customer's transactional profile. The IT system should enable the bank to maintain a centralized knowledge base of data, organized, for example, by business unit, legal entity within a larger group, and customer. It should be noted that although the guidelines stipulate that banks must have a system in place, this does not imply that a single IT tool can perform all of these functions; rather, the tools must be able to cooperate to provide the bank with an enterprise-level perspective of ML risk throughout the bank. Building on the data from risk assessments and client profiles, transaction monitoring systems' monitoring of

customer behavior is a vital component of mitigating money laundering risk.

- *Information Management:* Banks should keep records since one of the main goals of AML regulations is to generate documentation that allows law enforcement to track down the individuals who undertake financial transactions. When confirming the identity of a customer or beneficial owner, banks should keep a record of the documents they receive, whether they are photocopies or contain information from non-documentary sources, and they should also enter all CDD data into their IT system. It is necessary to regularly evaluate the CDD data, usually on a risk-based basis, to maintain accuracy and accuracy. Whether or not a report of suspicious conduct is filed, banks should document all decisions made regarding their investigations into unusual activity. As required by law, these records must be retained for at least five years after account closure. Relevant CDD records should not be deleted while an investigation is ongoing, even if the standard retention period has elapsed.

- *Suspicious Transaction Reporting and Asset Freezing:* By continuously monitoring accounts and transactions, banks can detect unusual activity, refer it to an internal review function, eliminate false positives, and report suspicious activity promptly and discreetly. Policies and procedures should clearly outline this process, and relevant staff members should be informed. The bank should take the proper action regarding the customer in cases where suspicious conduct has been discovered. This may involve increasing the customer's risk rating and determining whether to keep the relationship in place (either the account or the entire connection). For instance, when a customer has an outstanding loan and a checking account, it may be appropriate to stop the debt while keeping the account open. To identify connections that may need to be frozen, banks should screen potential new clients against relevant sanctions lists and review their existing portfolio against updated sanctions lists. Banks must

be able to properly freeze any assets identified during this process.

5.5 Emerging Technologies in AML Compliance

The rapid evolution of laundering techniques has outpaced conventional compliance mechanisms, making the adoption of emerging technologies indispensable for banks. Crypto-assets pose novel risks due to rapid cross-border transferability and the rise of decentralized finance. Regulators, including the FATF, have emphasized extending the Travel Rule to virtual asset service providers, underscoring the systemic implications for banks that facilitate crypto-related transactions. Blockchain technology simultaneously generates risk and opportunity. While anonymity-enhancing tools such as mixers facilitate laundering, blockchain analytics providers have enabled unprecedented transparency and traceability. Permissioned blockchain platforms further support secure data sharing, enhancing Know Your Customer (KYC) and Beneficial Ownership verification. Artificial intelligence (AI) and machine learning (ML) are increasingly deployed for transaction monitoring, anomaly detection, and adverse media screening. By processing vast, unstructured data in real time, AI reduces false positives and enhances Suspicious Transaction Reporting (STR) quality. However, challenges persist, including algorithmic bias, lack of explainability, and uneven regulatory acceptance. Together, these technologies are not stand-alone solutions but act as moderators that amplify the effectiveness of core compliance measures, thereby strengthening organizational resilience in the face of emerging laundering threats.

Conclusion

Money laundering remains a borderless and persistent threat, exploiting both weak jurisdictions and sophisticated financial hubs through complex transaction volumes and evolving technologies. Banks, as central actors in the financial system, continue to be primary targets across all stages of laundering. In today's technology-driven environment, criminals are quick to exploit innovations, making resilience a continuous challenge. This study underscores the importance of a risk-based, multi-dimensional AML framework grounded in core compliance measures such as the Risk-Based Approach, Customer Due Diligence (CDD), Suspicious Transaction Reporting (STR), and Beneficial Ownership transparency, reinforced by international standards (FATF, Basel, Wolfsberg, and EU AMLD). The proposed conceptual model highlights how technology adoption acts as a critical moderator, strengthening the effectiveness of compliance mechanisms and enabling banks to move from risk exposure to organizational resilience.

To safeguard legitimacy and trust, banks must prioritize robust AML programs that integrate risk assessment, internal controls, staff training, and independent auditing. By embedding resilience into compliance systems, financial institutions can not only mitigate reputational, operational, and legal risks but also adapt proactively to emerging laundering techniques in an era of rapid technological change.

References

[1]. Azman Aziz, Z. Z., & Md Daud, S. A. M. (2022). Customer's awareness, trust, discomfort and acceptance of anti-money laundering practices in Malaysian Banks. *Journal of Money Laundering Control,* 25(4), 864-881.

https://doi.org/10.1108/JMLC-08-2021-0087

[2]. Basel. (2023). *Basel AML Index 2023: 12th Public Edition Ranking Money Laundering and Terrorist Financing Risks around the World.* Retrieved from

https://baselgovernance.org/sites/default/files/2023-11/Basel%20AML%20Index%202023%2012th%20Edition.pdf

[3]. Bhure, L. (2003). *Money Laundering: An Insight Into The Dark World Of Financial Frauds,* Siddharth Publications.

[4]. FATF (2012-2025), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France. Retrieved from

https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

[5]. Jaffery, I. H., & Mughal, R. A. L. (2020). Money-laundering risk and preventive measures in Pakistan. *Journal of Money Laundering Control,* 23(3), 699-714.

https://doi.org/10.1108/JMLC-02-2020-0016

[6]. Juntunen, J., & Teittinen, H. (2023). Accountability in anti-money laundering–findings from the banking sector in Finland. *Journal of Money Laundering Control,* 26(2), 388-400.

https://doi.org/10.1108/JMLC-12-2021-0140

[7]. Madinger, J. (2011). *Money laundering: A Guide for Criminal Investigators,* CRC Press.

[8]. Nations, U. (2000). Summary of the United Nations convention against transnational organized crime and protocols thereto. *Trends in Organized Crime,* 5(4), 11-21.

https://doi.org/10.1007/s12117-000-1044-5

[9]. Rose, K. J. (2020). De-risking or recontracting–the risk dilemma of EU money laundering regulation. *The Journal of Risk Finance,* 21(4), 445-458.

https://doi.org/10.1108/JRF-12-2019-0237

[10]. Sathye, M., & Islam, J. (2011). Adopting a risk-based approach to AMLCTF compliance: the Australian case. *Journal of Financial Crime,* 18(2), 169-182.

https://doi.org/10.1108/13590791111127741

[11]. Sullivan, K. (2023). *Anti–Money Laundering in a Nutshell,* Apress.

[12]. Sundarakani, S., & Ramasamy, M. (2013). Consequences of money laundering in banking sector. *Jurnal Teknologi (Sciences & Engineering),* 64(2).

https://doi.org/10.11113/jt.v64.2243

[13]. UNODC. (2011). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes.* Retrieved from

https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

[14]. Viritha, B., Mariappan, V., & Venkatachalapathy, V. (2015). Combating money laundering by the banks in India: compliance and challenges. *Journal of Investment Compliance,* 16(4), 78-95.

https://doi.org/10.1108/JOIC-07-2015-0044

[15]. Zakaria, N. B., Mohamed, N., & Marzukai, N. (2022). Determinant of compliance perceptions among bank officers towards anti-money laundering. *Universal Journal of Accounting and Finance,* 10(2), 457-464.

https://doi.org/10.13189/ujaf.2022.100210

ABOUT THE AUTHORS

Zmarialy Yousufi is a Ph.D. Research Scholar at the Institute of Management in Kerala (IMK), University of Kerala, Thiruvananthapuram, Kerala, India. His doctoral thesis deals with anti-money laundering. He holds a Master's and a Bachelor's degree in Management (MBA and BBA), specializing in Accounting and Finance. He has worked as an Anti-Money Laundering and Combating Terrorist Financing (AML/CTF) Examiner with the Regulatory and Supervisory Division of Da Afghanistan Bank (Central Bank of Afghanistan). He has worked in different operations positions at Azizi Bank.

Dr. P. N. Harikumar is working as a Professor in the Department of Commerce, School of Business Management and Legal Studies, University of Kerala, India. He holds a Ph.D. in Commerce, a Ph.D. in Management Studies (Marketing), and an M.Com. (Finance), an M.Phil. (Finance), and an MBA (HR and Marketing). He is one of the secretaries of the Commerce and Management Association of India (CMAI), an executive member of the Punjab Commerce and Management Association (PCMA), and a life member of the Indian Commerce Association (ICA) and the Indian Accounting Association (IAA). He is the Chief Editor of several international publications, including Commerce and Management Explorer, Kegees Journal of Social Science, Sivasailam Journal of Social Science, and Sivasailam Business Researcher. He has published 165 research papers in national and international journals. Moreover, he has published 56 books relating to commerce and management subjects. Under his guidance, 21 PhDs have been awarded, and eight research scholars are working at Kerala University. He is a Chief Resource Person in the UGC-Academic Staff Colleges of Mysore University, Bangalore University, SV University, Thiruppathi, Kannur University, and the University of Kerala for refresher courses in commerce and management and other subjects of social science. He is a member of the BOS of Commerce (PG) and Management (PG) at the University of Kerala, the BOS of Management (PG) at Calicut University and Kannur University, and a faculty member of the Management of Mahatma Gandhi University. He is also a member of the Research Committee of Mahatma Gandhi University and Kannur University, Kerala, India.