



# AHMADU BELLO UNIVERSITY LAW JOURNAL

FACULTY OF LAW

AHMADU BELLO UNIVERSITY, ZARIA - NIGERIA.

website: <https://abulj.org.ng> | e-mail: [abulj@abu.edu.ng](mailto:abulj@abu.edu.ng)

## AN APPRAISAL OF THE ROLE OF ANTI-MONEY LAUNDERING LAWS IN COMBATING FINANCIAL CRIMES AND TERRORIST FINANCING AMIDST GLOBAL GEOPOLITICAL TURMOIL

LATEEFAT ADEOLA BELLO\*

---

### Abstract

In today's rapidly evolving global financial landscape, the rise in financial crimes and terrorist financing continues to threaten the economic and national security of nations. This paper aims to assess the effectiveness of Anti-Money Laundering (AML) laws in addressing these threats, particularly amid increasing geopolitical instability. The primary objectives are to examine how current AML frameworks respond to the complex tactics used by criminal and terrorist networks, analyse the role of international cooperation, and explore the potential of emerging technologies in enhancing financial oversight. Employing a doctrinal research approach based on a thorough review of academic literature, policy documents, and regulatory reports, the paper evaluates the strengths and weaknesses of existing AML regimes. The analysis revealed that financial crimes are becoming more transnational, exploiting regulatory gaps, weak jurisdictions, and global conflicts to transfer illicit funds undetected. It also finds that many current AML mechanisms struggle to keep pace with the evolving strategies of criminal and terrorist actors. The paper highlights the urgent need for stronger international cooperation among financial institutions, regulators, and law enforcement agencies. It also advocates for the strategic use of innovative technologies such as blockchain analytics, machine learning, and artificial intelligence to enhance real-time detection and reduce human oversight errors. In conclusion, the paper recommends a multi-layered approach that is, strengthening AML legislation, investing in cross-border intelligence sharing, and

---

\* Senior Lecturer, Department of Commercial Law, Faculty of Law, Ahmadu Bello University, Zaria, Nigeria, +2348031530751 [attorney4real@yahoo.com](mailto:attorney4real@yahoo.com) [blateefat@abu.edu.ng](mailto:blateefat@abu.edu.ng)

modernising compliance systems through technological integration. These actions are vital for protecting global financial integrity and disrupting the financial support networks of criminal and terrorist organisations in an era marked by geopolitical uncertainty.

---

**Key Words:** Anti-Money Laundering (AML), terrorist financing, geopolitical instability, blockchain, artificial intelligence.

## 1.1 Introduction

In today's interconnected financial world, the scale and sophistication of money laundering and terrorist financing have grown exponentially, posing significant threats to global economic stability, national security, and the integrity of legitimate financial systems.<sup>1</sup> With the increasing integration of global markets and the digitisation of financial flows, criminal and terrorist networks have gained unprecedented ability to move illicit funds across borders, often undetected and unregulated. This reality has become even more complex in the wake of persistent geopolitical turmoil, including wars, sanctions, refugee crises, and political instability, which collectively create loopholes that these actors exploit.<sup>2</sup> This paper sets out to critically appraise the effectiveness of Anti-Money Laundering (AML) laws in preventing financial crimes and curbing terrorist financing, particularly in the context of global political instability. The aim is to assess whether current AML regimes are fit for purpose in addressing the evolving patterns of illicit finance, and to explore how geopolitical conditions have reshaped the enforcement landscape.

The objectives of this study are to:

1. To identify key challenges in the implementation and enforcement of AML laws at both national and international levels.

---

<sup>1</sup> United Nations Office on Drugs and Crime (UNODC), *Money-Laundering and Globalisation*, 2022.

<sup>2</sup> E. Baker, "The Politics of Non-Cooperation: Geopolitics and Illicit Finance" (2022) *Journal of Financial Crime* Vol. 29(4).

2. examine how geopolitical instability and technological advancements affect the ability of states to monitor and regulate illicit financial flows; and
3. Propose pragmatic reforms that are legal, institutional, and technological, that can enhance the robustness of AML systems.

The research problem arises from the widening gap between the sophistication of illicit financial networks and the capacity of legal frameworks to address them. Despite international instruments such as the Financial Action Task Force (FATF) Recommendations and the United Nations Conventions, enforcement remains inconsistent, data sharing is limited, and many countries still lack the technical capacity to meet international standards.<sup>3</sup> Criminal syndicates and terrorist groups continue to use shell companies, anonymous cryptocurrencies, and safe-haven jurisdictions to evade detection.<sup>4</sup>

This paper adopts a qualitative doctrinal methodology, relying on a detailed review of international treaties, Nigeria's Money Laundering (Prevention and Prohibition) Act 2022, academic literature, and institutional reports from bodies such as FATF and the Basel Institute.<sup>5</sup> Comparative legal analysis is also employed, drawing on case studies from both developed and developing jurisdictions to contextualise the enforcement challenges.

Preliminary findings suggest that while legislative progress has been made, especially in aligning with FATF standards, significant gaps persist in enforcement, regulatory independence, inter-agency collaboration, and technological adaptation.<sup>6</sup> The paper also identifies that ongoing geopolitical

---

<sup>3</sup> Financial Action Task Force (FATF), *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, 2022.

<sup>4</sup> Basel Institute on Governance, *AML Index 2023: Ranking Money Laundering and Terrorist Financing Risks Around the World*

<sup>5</sup> Nigeria, *Money Laundering (Prevention and Prohibition) Act, 2022*; see also OECD and FATF reports on jurisdictional compliance.

<sup>6</sup> *Ibid.* FATF Mutual Evaluation Reports; World Bank, *Strengthening Financial Integrity*, 2021.

tensions reduce the effectiveness of international cooperation, as mutual legal assistance and data exchange are often constrained by distrust, political rivalries, or differing priorities.<sup>7</sup> In response, this paper recommends a multidimensional approach. This includes strengthening international cooperation through enforceable cross-border frameworks, enhancing the use of fintech and AI-based transaction monitoring tools, building technical capacity in developing economies, and promoting regional AML taskforces. Furthermore, national laws must be regularly updated to reflect global best practices, emerging risks, and technological shifts.<sup>8</sup> Ultimately, this paper contributes to the growing body of research advocating for a more coordinated, adaptive, and technology-driven response to illicit financial flows, one that recognises the global and political nature of money laundering and terrorist financing in the 21st century.

## **1.2 Evolution and Fundamentals of Anti-Money Laundering Laws**

The evolution of Anti-Money Laundering (AML) laws reflects the ongoing global response to the rising complexity of financial crimes and their far-reaching socio-economic and security implications. From their early beginnings as isolated domestic responses to criminal financial behaviour, AML frameworks have transformed into an interconnected and sophisticated global regime, driven by the need to counter not only money laundering but also the financing of terrorism and proliferation of weapons. A critical turning point in this evolution was the establishment of the Financial Action Task Force (FATF) in 1989 by the G7 nations. The FATF's initial mandate was to examine and develop measures to combat money laundering, which resulted in the issuance of the Forty Recommendations, a comprehensive set of guidelines for countries to implement

---

<sup>7</sup> J. Sharman, *The Despot's Guide to Wealth Management: On the International Campaign against Grand Corruption* (2017), Cornell University Press

<sup>8</sup> R. Levi and S. Gilmore, "Harnessing Blockchain for Financial Transparency" (2021) *Law, Innovation and Technology* Vol. 13.

effective AML regimes.<sup>9</sup> In the wake of the September 11, 2001, attacks, FATF expanded its focus to include Counter Financing of Terrorism (CFT), adding nine Special Recommendations, which have since been integrated into its revised Forty Recommendations.<sup>10</sup> These instruments have since served as the global standard for AML/CFT policy, influencing both national laws and institutional practices.<sup>11</sup>

Over the years, AML laws have evolved significantly to keep pace with emerging threats—including cyber-enabled financial crime, crypto-asset misuse, and the exploitation of offshore structures. Regulatory frameworks have shifted from mere reactive enforcement to proactive risk-based approaches.<sup>12</sup> Many jurisdictions now mandate ongoing customer due diligence (CDD), politically exposed person (PEP) screenings, and enhanced due diligence (EDD) for high-risk clients or regions. Technological advancements, such as transaction monitoring systems and AI-driven compliance tools, are now integral to AML enforcement.

At their core, AML laws are designed to prevent the processing of funds derived from illegal activities such as drug trafficking, corruption, fraud, human trafficking, arms smuggling, and tax evasion. The aim is to detect, disrupt, and deter the process of "cleaning" these illicit funds, which criminals attempt to integrate into the legal economy. In this way, AML laws protect financial institutions from being exploited and help preserve the credibility of the global

---

<sup>9</sup> (FATF)Financial Action Task Force (FATF), The Forty Recommendations, 1990 (updated 2022) is an autonomous intergovernmental organisation dedicated to formulating and advancing policies that safeguard the global financial system from threats such as money laundering, terrorist financing, and the proliferation of weapons of mass destruction. The FATF's Recommendations are widely acknowledged as the international benchmark for anti-money laundering (AML) and counter-terrorist financing (CFT) standards.

<sup>10</sup> FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2022).

<sup>11</sup> *ibid.*

<sup>12</sup> Basel Institute on Governance, Basel AML Index 2023.

financial system. The fundamentals of AML laws rest on several core components:

Customer Due Diligence (CDD), which requires financial institutions and designated non-financial businesses and professions (DNFBPs) to verify the identity of clients and understand the nature of their business relationships;

Suspicious Activity Reporting (SAR), which obligates institutions to report transactions that may indicate money laundering or terrorist financing;

Record-Keeping, requiring the retention of transactional and identity documentation for a defined period (often five years); and

Ongoing Monitoring, through automated systems or manual review of client behaviour and transaction patterns.<sup>13</sup>

Enforcement mechanisms differ across jurisdictions, but they generally include a combination of administrative, civil, and criminal penalties. Supervisory and regulatory bodies—such as Financial Intelligence Units (FIUs), central banks, financial conduct authorities, and law enforcement agencies—are responsible for ensuring compliance, conducting inspections, and pursuing violations.

In Nigeria, for example, the Nigerian Financial Intelligence Unit (NFIU), the Central Bank of Nigeria (CBN), and the Economic and Financial Crimes Commission (EFCC) collaborate to enforce AML standards and investigate financial misconduct under laws such as the Money Laundering (Prevention and Prohibition) Act, 2022.

On a global scale, international cooperation has become a cornerstone of effective AML enforcement. The FATF continues to play a pivotal coordinating role, conducting mutual evaluations of member states and publishing grey and blacklists of non-compliant jurisdictions. Regional bodies such as the Inter-

---

<sup>13</sup> UNODC, Toolkit for Anti-Money Laundering Measures, 2022.

Governmental Action Group Against Money Laundering in West Africa (GIABA) serve similar roles within their respective jurisdictions.<sup>14</sup> These organisations foster cross-border information sharing, capacity building, and harmonisation of legal standards.

In today's digital age marked by cryptocurrencies, online banking, and increasing geopolitical tensions, AML laws are more important than ever. The abuse of financial systems by transnational criminal and terrorist networks underscores the need for legal frameworks that are adaptive, collaborative, and technology-driven. Beyond protecting the financial sector, AML laws contribute to national security, economic development, and the rule of law.

### **1.3 The nexus between Financial Crimes and Terrorist Financing**

Financial crimes and terrorist financing pose significant risks to global security and economic stability. They include a variety of illegal actions such as money laundering, fraud, corruption, tax evasion, and cybercrime. Money laundering makes it appear legitimate, which is frequently accomplished through sophisticated financial transactions. Ponzi schemes, insider trading, and identity theft are examples of fraudulent schemes that take advantage of flaws in financial institutions to illegally obtain income or assets. Corruption, bribery, and embezzlement undermine public and private institutions, erode trust in governance, and impede economic progress.

Terrorist organisations rely on a variety of funding sources to continue their operations and perpetrate atrocities, with terrorist finance including financial support for recruiting, training, and weapon procurement. Financial crimes such as money laundering and fraud can contribute to terrorist financing by making it

---

<sup>14</sup>GIABA, Annual Report on AML/CFT Trends in West Africa, 2023.

easier to transfer and conceal funds.<sup>15</sup> The interconnectedness of criminal networks and terrorist organisations challenges law enforcement and regulatory operations. Financial crimes and terrorist financing not only jeopardise the global financial system's integrity, but they also undermine investor confidence and stymie economic growth. Illicit financial operations fuel corruption, instability, and social discontent, aggravating geopolitical tensions and undermining governance systems.<sup>16</sup> Terrorist attacks funded through illegal channels not only result in loss of life and property but also have far-reaching geopolitical consequences, such as increased security concerns, instability, and interruptions to international trade. Understanding how financial crimes and terrorist financing are interwoven is critical for building successful counterterrorism policies in the face of persistent geopolitical conflicts.

#### **1.4 Nature and scope of financial crimes and Impact on Global Security and Stability**

Understanding the multidimensional nature of financial crimes is essential for developing comprehensive strategies to prevent, detect, and prosecute unlawful financial activity. These crimes not only threaten the integrity of financial institutions but also undermine public trust, economic growth, and national security. Financial crimes encompass a wide array of illegal activities that exploit systemic vulnerabilities for personal or organisational gain—ranging from money laundering and fraud to terrorist financing and insider trading. Their complex and often transnational nature poses significant challenges to enforcement agencies, regulators, and policymakers.<sup>17</sup>

---

<sup>15</sup> Basile, M. (2004). Terrorism Financing: Roots and Trends of Saudi Terrorism Financing. *Journal of International Affairs*, 57(2), 63-80.

<sup>16</sup> FATF (2019), *Terrorist Financing Risk Assessment Guidance*, FATF, Paris, [www.fatf-gafi.org/publications/methodsandtrends/documents/Terrorist-Financing-Risk-Assessment-Guidance.html](http://www.fatf-gafi.org/publications/methodsandtrends/documents/Terrorist-Financing-Risk-Assessment-Guidance.html).

<sup>17</sup> FATF, *Money Laundering and Terrorist Financing: Definitions and Challenges*, 2022.



Effectively combating financial crimes requires a clear understanding of their mechanics, motivations, and implications. Such understanding forms the foundation for enforcing robust regulations, designing risk-sensitive compliance systems, and fostering international cooperation. Moreover, in an era of digital finance and geopolitical uncertainty, identifying and addressing these threats is more critical than ever to ensure economic resilience and social stability.<sup>18</sup> Below is an overview of several key types of financial crimes, each of which illustrates how illicit actors exploit financial systems and highlights the regulatory and enforcement challenges they present.

Money laundering is the process of disguising the source of unlawfully obtained funds to make them appear genuine, which is commonly accomplished through the placement, layering, and integration stages. Criminal proceeds from operations such as drug trafficking, corruption, fraud, and organised crime are laundered using banks, shell businesses, and virtual currencies. Annually, trillions of dollars are laundered around the world, weakening the integrity of the financial system and facilitating more illegal activity.<sup>19</sup>

Fraud refers to many fraudulent techniques used to illegally obtain money or assets by deception, misrepresentation, or manipulation. Investment fraud, Ponzi schemes, identity theft, credit card fraud, and phishing scams are among examples. Fraudsters use technology and social engineering to target individuals, businesses, and financial institutions, causing enormous financial losses and degradation of confidence.<sup>20</sup>

Corruption involves abusing entrusted power for personal gain, often through bribery, embezzlement, kickbacks, or nepotism. It undermines the rule of law,

---

<sup>18</sup> UNODC, Global Report on Financial Crime and Corruption, 2023.

<sup>19</sup> United Nations Office on Drugs and Crime (UNODC). (2022). Money Laundering. Retrieved from <https://www.unodc.org/unodc/en/money-laundering/overview.html>

<sup>20</sup> Financial Action Task Force (FATF). (2022). Fraud. Retrieved from <https://www.fatf-gafi.org/about/fraud/> accessed June 15 2025

distorts market competition, and diverts resources from essential services, hindering economic development and fostering inequality. Both public and private sector entities can be complicit, leading to reduced investor confidence, political instability, and social unrest.<sup>21</sup>

Cybercrime refers to illegal actions carried out through digital platforms and networks that target sensitive information, financial assets, and essential infrastructure. Examples include hacking, malware assaults, ransomware, and data breaches, which result in financial losses, reputational damage, and service disruptions.<sup>22</sup>

The development of cybercrime creates enormous hurdles for law enforcement and regulatory bodies, necessitating increased cybersecurity measures and international cooperation. These criminal actions undermine trust in institutions, stifle economic growth, and create social instability. They also muddle the distinction between organised crime and terrorism, hindering law enforcement efforts. Furthermore, they fund activities that undermine state sovereignty and contribute to global strife. Addressing these concerns would necessitate international cooperation and strong initiatives to combat and maintain the integrity of the global financial system.

### **1.5 Escalating Geopolitical Tensions Worldwide and Influence on Financial Systems and Regulatory Environments.**

Geopolitical turbulence, caused by international conflicts, disagreements, and power struggles, has a substantial impact on financial crime and terrorist financing. Territorial disputes, ideological divisions, economic rivalries, and regional power dynamics are all factors that contribute to geopolitical tensions, as

---

<sup>21</sup> Transparency International Corruption Perceptions Index. (2022). Retrieved from <https://www.transparency.org/en/cpi/2021/> accessed June 15 2025

<sup>22</sup> Federal Bureau of Investigation (FBI). Cybercrime (2022). Available at <https://www.fbi.gov/investigate/cyber> Retrieved November 2024

evidenced by current hostilities in the Middle East, Eastern Europe, and the South China Sea.<sup>23</sup> This upheaval exacerbates uncertainty and market volatility, allowing criminal and terrorist organisations to exploit legal loopholes and further their agendas. It destabilises financial institutions and regulatory settings, undermining investor trust and increasing vulnerabilities to money laundering, fraud, and corruption. Weak governance and inefficient law enforcement exacerbate these issues, particularly in conflict-affected areas where illicit money operations thrive, prolonging humanitarian crises and hampering peace-building efforts. Illicit finances fuel conflicts, perpetuate violence, and undermine stability and development initiatives.<sup>24</sup> To address these implications, proactive actions are needed, including enhancing AML/CFT frameworks, boosting regulatory monitoring, and encouraging openness and accountability. Multilateral initiatives, such as the FATF, are critical for coordinating efforts to address financial crimes in crisis zones. Investments in conflict prevention, peacebuilding, and sustainable development are critical to addressing root causes and promoting long-term stability. Policymakers must recognise the impact of geopolitical turbulence on financial crimes and terrorist financing to develop comprehensive plans that minimise risks and defend the integrity of the global financial system.<sup>25</sup>

Geopolitical conflicts have a considerable impact on financial systems and laws, resulting in disruption, volatility, and problems. Investors respond with uncertainty and risk aversion, causing volatility in asset prices and currency values. Investor confidence may decline, resulting in capital flight and market instability. Regulatory compliance and risk management grow more difficult as institutions negotiate geopolitical threats. Regulatory agencies may implement

---

<sup>23</sup> Ahmet Kaya, How are Geopolitical Risks Affecting the World Economy(2024)? Available at <https://www.economicsobservatory.com/how-are-geopolitical-risks-affecting-the-world-economy>, available at 20 Jan 2025

<sup>24</sup> Council on Foreign Relations. (2022). Global Conflict Tracker. Retrieved from <https://www.cfr.org/global-conflict-tracker>.

<sup>25</sup> Financial Stability Board (FSB), Geopolitical Tensions and Financial Stability(2022). Retrieved from <https://www.fsb.org/work-of-the-fsb/>

stronger transaction restrictions and change standards to reflect this. Compliance with sanctions and anti-money laundering legislation becomes increasingly difficult. Uncertainties in trade policies hurt trade financing and supplier chains. Geopolitical pressures underscore the importance of international cooperation in managing cross-border hazards. Multilateral organisations, such as the Financial Stability Board and the IMF, are critical in establishing policy responses. Recognising these factors allows policymakers to make proactive efforts to improve resilience and stability in global financial markets.<sup>26</sup>

### **1.6 Regulatory Complexity and Compliance Burden**

Escalating geopolitical tensions pose a multidimensional challenge to anti-money laundering operations, complicating regulatory compliance, raising financial risks, and eroding international collaboration.<sup>27</sup> It also adds regulatory complexity for financial institutions, which must navigate changing anti-money laundering (AML), counter-financing of terrorism (CFT), and sanctions legislation across many jurisdictions.<sup>28</sup> Compliance with international standards, such as those established by the Financial Action Task Force (FATF), becomes increasingly difficult, requiring increased due diligence, risk assessment, and reporting requirements.<sup>29</sup> Stricter controls on cross-border transactions and client surveillance may be implemented to prevent geopolitical risks, increasing financial institutions' compliance burden.<sup>30</sup> Similarly, in the face of geopolitical

---

<sup>26</sup> International Monetary Fund (IMF). 2022. Global Financial Stability Report. Retrieved from <https://www.imf.org/en/Publications/GFSR>

<sup>27</sup> Howard Cooper and Oliver Sten, How Geopolitical Tensions Fuel Financial Crime, Kroll, Financial Crime Report, 2025, retrieved from [https://www.kroll.com/en/publications/financial-crime-report-2025/how-geopolitical-tensions-fuel-financial-crime?utm\\_source=chatgpt.com](https://www.kroll.com/en/publications/financial-crime-report-2025/how-geopolitical-tensions-fuel-financial-crime?utm_source=chatgpt.com) accessed 28 July 2025

<sup>28</sup> Idenfo Direct, "The Impact of Geopolitical Changes on AML/KYC: Navigating a Shifting Global Landscape," 2025. Retrieved from [https://www.idenfodirect.com/articles/the-impact-of-geopolitical-changes-on-aml-kyc-navigating-a-shifting-global-landscape/?utm\\_source=chatgpt.com](https://www.idenfodirect.com/articles/the-impact-of-geopolitical-changes-on-aml-kyc-navigating-a-shifting-global-landscape/?utm_source=chatgpt.com) Accessed 20 July 2025

<sup>29</sup> Ibid

<sup>30</sup> FATF, "Complex Proliferation Financing and Sanctions Evasion Schemes," June 20 2025.

tensions, illicit actors may exploit regulatory gaps and clever evasion methods to bypass AML/CFT requirements. They may employ technology to launder funds, anonymise transactions, and exploit weaknesses in digital platforms, posing further challenges to AML operations. Furthermore, geopolitical disputes can stymie information transmission and collaboration between law enforcement and regulatory organisations across borders, diminishing the effectiveness of joint investigations and asset recovery efforts.

In a related development, diplomatic tensions and political rivalry may limit international collaboration on AML/CFT initiatives, while country-specific AML/CFT regime fragmentation could create gaps in the global battle against money laundering and terrorist funding.<sup>31</sup> Geopolitical tensions can also strain resources and stymie capacity-building initiatives in conflict-affected areas, raising vulnerability to illicit financial activity. Regardless of bureaucratic constraints and donor fatigue, effectively resolving AML/CFT concerns needs persistent efforts and collaboration among stakeholders.<sup>32</sup>

### **1.7 Emerging tactics and strategies employed by criminal organisations**

In a related development, diplomatic tensions and political rivalry may limit international collaboration on AML/CFT initiatives, while country-specific AML/CFT regime fragmentation could create gaps in the global battle against money laundering and terrorist funding.

1. Geopolitical tensions can also strain resources and stymie capacity-building initiatives in conflict-affected areas, raising vulnerability to illicit financial activity. Regardless of bureaucratic constraints and donor fatigue, effectively resolving AML/CFT concerns needs persistent efforts and collaboration among stakeholders.

---

<sup>31</sup> IMF, "International Cooperation in Combating the Financing of Terrorism,

<sup>32</sup> Wolfsberg Group, Anti-Money Laundering(2022). Retrieved from <https://www.wolfsberg-principles.com/anti-money-laundering>. Accessed 28 July 2024.

2. Criminal organisations' involvement in cybercrime, particularly ransomware assaults in which they encrypt victims' data and demand cryptocurrency ransom payments, allowing criminals to remain anonymous and supporting illicit cash flows.
3. Criminals create shell businesses or front organisations to conceal the ownership and control of illicit funds, participating in legitimate-appearing operations to mask unlawful proceeds.
4. Criminals employ systems such as hawala and hundi to transfer money across borders without leaving a paper trace, depending on trust networks and working outside of established banking channels. In reaction to legislative measures and technical improvements, terrorist groups have also adjusted their funding mechanisms by:

### **1.8 Regulatory responses and policy measures**

To counteract the activities and the effect of the laundering activities of terrorist groups. The following Key approaches are

1. Authorities continuously update regulations to address emerging threats. This involves adopting risk-based approaches to combat money laundering and terrorist financing across various sectors like banking, cryptocurrency, and trade.
2. Know Your Customer (KYC) and enhanced due diligence (EDD) requirements are reinforced to ensure robust customer identification and verification, especially in high-risk sectors. Enhanced screening helps uncover suspicious activities and entities linked to criminal or terrorist financing.
3. Regulatory agencies, law enforcement, and financial institutions enhance collaboration to combat illicit financial activities. Cross-border

cooperation aids in timely intelligence exchange, aiding in identifying and disrupting criminal networks and terrorist financing operations.

4. 1. Regulatory authorities closely monitor and supervise financial institutions and designated non-financial businesses. Regular audits assist in identifying compliance flaws, allowing for enforcement actions against noncompliance.
5. 2. Leverage technology and creativity to improve AML/CFT capability. This incorporates advanced analytics, artificial intelligence, and machine learning algorithms to detect suspicious transactions and better monitor developing threats.
6. International regulatory agencies work to develop common standards and guidelines for anti-money laundering and counter-terrorism measures. Multilateral organisations like the FATF foster dialogue, encourage convergence, and check global compliance. To disrupt criminal networks and promote compliance, authorities apply sanctions and fines on persons, businesses, and jurisdictions that engage in unlawful financial activity. PPPs enable collaboration among government agencies, financial institutions, and industry stakeholders, strengthening the collective response to financial crimes and terrorist financing. Authorities can increase their AML/CFT efforts. Authorities can increase their AML/CFT efforts, mitigate risks, and protect the integrity of the global financial system.

### **1.9 Importance of collaborative efforts in combating financial crimes**

International cooperation and coordination are indispensable for addressing the inherently transnational nature of financial crimes and terrorist financing. The Financial Action Task Force (FATF) provides a globally recognised framework through its Recommendations, which guide countries in structuring their

AML/CFT systems and fostering international collaboration.<sup>33</sup> Member states engage in mutual evaluations—peer-reviewed assessments of compliance and effectiveness that identify legal and operational gaps and offer targeted recommendations for improvement.<sup>34</sup> Countries also enter into bilateral agreements to support mutual legal assistance, intelligence sharing, and joint investigations. Such partnerships enhance enforcement capabilities, enabling law enforcement agencies to combat cross-border financial crime more effectively.<sup>35</sup>

A critical enabler of effective coordination is the Egmont Group of Financial Intelligence Units (FIUs). Founded in 1995, this international network facilitates secure, structured exchange of financial intelligence—including Suspicious Activity Reports (SARs)—among FIUs worldwide.<sup>36</sup> It's a secure platform, the Egmont Secure Web that ensures confidentiality and standardisation across participating jurisdictions.<sup>37</sup> In addition, countries establish joint operations and task forces to target organised criminal and terrorist networks operating across borders. These interagency collaborations foster real-time coordination of intelligence, investigations, and prosecutions, improving operational effectiveness.<sup>(6)</sup> Through these mechanisms, FATF mutual evaluations, bilateral agreements, Egmont Group coordination, and joint enforcement initiatives, international collaboration strengthens the global fight against money laundering and terrorist financing. It promotes transparency, builds capacity, and ensures that

---

<sup>33</sup> FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2022).

<sup>34</sup> FATF, "Mutual Evaluations: In-Depth Country Analysis and Peer Review Process

<sup>35</sup> GIABA, *The Importance of Effective AML/CFT Regimes to West African Economies* (2023)

<sup>36</sup> Egmont Group, *Connecting Financial Intelligence Units Worldwide*. Retrieved from [https://kyrosaml.com/egmont-group-of-financial-intelligence-units/?utm\\_source=chatgpt.com](https://kyrosaml.com/egmont-group-of-financial-intelligence-units/?utm_source=chatgpt.com) Accessed 29 July 2025

<sup>37</sup> Egmont Group Strategic Plan 2022–2027 highlighting collaborative task forces and operations Retrieved from <https://ripjar.com/blog/4-key-takeaways-for-fius-from-the-egmont-groups-strategic-plan-2022-2027/?utm> Accessed 30 July 2025.



legal and operational regimes stay aligned with evolving threats and vulnerabilities.

Collaborative efforts are essential in combating financial crimes, especially given their increasingly transnational nature. Illicit financial flows such as money laundering, terrorist financing, and corruption frequently transcend national borders, often exploiting jurisdictional loopholes and regulatory inconsistencies.<sup>38</sup> In this context, both regional organisations and public-private partnerships (PPPs) have emerged as crucial pillars in the global anti-money laundering and counter-terrorist financing (AML/CFT) framework.

Regional bodies such as the European Union (EU), the Association of Southeast Asian Nations (ASEAN), and the Caribbean Financial Action Task Force (CFATF) have made significant contributions by fostering regional dialogue, building institutional capacity, and coordinating AML/CFT policies.<sup>39</sup> These regional frameworks offer member states the opportunity to harmonise their legal regimes, share intelligence, and tackle region-specific vulnerabilities through collective action.

In parallel, public-private partnerships bring together government agencies, financial institutions, and industry experts to promote strategic coordination in AML/CFT implementation. Through PPPs, stakeholders can share typologies, red flag indicators, and suspicious activity reports (SARs), enabling a more targeted response to emerging threats.<sup>40</sup> These partnerships also encourage innovation—particularly in the application of fintech and artificial intelligence—to strengthen

---

<sup>38</sup> FATF, *Money Laundering & Terrorist Financing – A Global Threat* (2023), available at: <https://www.fatf-gafi.org>.

<sup>39</sup> Caribbean Financial Action Task Force (CFATF), *Mutual Evaluation Reports and Strategic Implementation Planning*, available at: <https://www.cfatf-gafic.org>.

<sup>40</sup> FATF, *Public-Private Partnerships in AML/CFT Efforts: Guidance Report* (July 2021), retrieved from <https://www.fatf-gafi.org/publications>.

transaction monitoring and risk detection systems.<sup>41</sup> Furthermore, collaborative mechanisms allow countries to leverage collective resources, technical expertise, and investigative tools that might otherwise be unavailable, especially to developing or resource-constrained nations.<sup>42</sup> By sharing best practices and offering mutual technical assistance, such partnerships empower countries to build more robust AML/CFT systems and meet international compliance obligations.<sup>43</sup>

The timely and accurate exchange of financial intelligence through collaborative channels significantly enhances the detection and disruption of criminal financial networks.<sup>44</sup> Inter-agency and cross-border cooperation also promote a coordinated enforcement regime, closing the regulatory gaps that financial criminals exploit. When countries apply global standards consistently, it deters illicit actors, strengthens the integrity of financial systems, and protects the global economy from systemic abuse.<sup>45</sup> Thus, regional and public-private collaboration is no longer optional; it is an imperative. Only through sustained international, regional, and bilateral partnerships can the global community effectively detect, deter, and dismantle the complex web of modern financial crimes.

Public-private partnerships (PPPs) are an increasingly vital element in the global effort to combat financial crimes. These collaborative frameworks bring together government authorities, financial institutions, and private sector stakeholders to

---

<sup>41</sup> Egmont Group, Enhancing FIU Collaboration through Technology and Innovation, Annual Report 2022–2023, p. 17.

<sup>42</sup> GIABA, Capacity Building for AML/CFT Compliance in West Africa (2023), available at: <https://www.giaba.org>.

<sup>43</sup> World Bank, Developing Effective AML/CFT Frameworks for Low-Income Countries (2022), Retrieved from <https://www.worldbank.org>. Accessed 30 July 2025

<sup>44</sup> Egmont Group of FIUs, Secure Information Sharing and SAR Exchange via the Egmont Secure Web (ESW), retrieved from <https://egmontgroup.org>. Accessed 30 July 2025

<sup>45</sup> FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (Updated March 2022), available at: <https://www.fatf-gafi.org>.

share timely information, co-develop innovative solutions, and execute joint initiatives aimed at detecting and disrupting illicit financial activities.<sup>46</sup> Through such partnerships, regulatory compliance is strengthened, risk-based approaches are enhanced, and systemic vulnerabilities within financial institutions are reduced.

In an era of rapid technological transformation, financial criminals continuously adapt by exploiting emerging tools such as cryptocurrencies, anonymising technologies, and cyber-enabled fraud schemes.<sup>47</sup> The borderless nature of digital financial platforms makes it increasingly difficult for traditional law enforcement and regulatory agencies to respond in isolation. PPPs allow for the fusion of intelligence, enabling governments and financial institutions to stay ahead of evolving threats by sharing typologies, real-time alerts, and analytical trend reports.<sup>48</sup> For instance, in countering the misuse of digital currencies or addressing terrorist financing, the pooling of resources, technical know-how, and investigative capacity across sectors provides a more resilient and holistic defence.<sup>49</sup> Public-private cooperation also fosters regulatory innovation, improving customer due diligence (CDD) mechanisms and the development of advanced transaction monitoring systems powered by artificial intelligence and machine learning.<sup>50</sup> By creating trusted communication channels and aligning

---

<sup>46</sup> FATF, Public-Private Partnerships: Enhancing the Effectiveness of AML/CFT Efforts (2021), available at: <https://www.fatf-gafi.org/publications>.

<sup>47</sup> Europol, Cryptocurrencies and Criminal Finances: The Impact of Technology on Money Laundering and Terrorist Financing, (2022), available at: <https://www.europol.europa.eu>.

<sup>48</sup> World Economic Forum, The Role of Public-Private Partnerships in Tackling Financial Crime, (2023), available at: <https://www.weforum.org>.

<sup>49</sup> GIABA, Combatting the Abuse of Virtual Assets in West Africa (2022), available at: <https://www.giaba.org>

<sup>50</sup> Egmont Group, The Role of Emerging Technologies in AML/CFT Supervision and Intelligence, (2022), available at: <https://egmontgroup.org>.

incentives, PPPs are not only effective in bolstering compliance but also in reinforcing the overall integrity and security of the international financial system.

### **1.10 Role of intergovernmental organisations and multilateral agreements**

Multilateral agreements are essential in strengthening the legal and regulatory frameworks needed to tackle financial crimes, such as money laundering and terrorist financing. These agreements foster international cooperation, enabling countries to work together across borders to address these complex issues. Intergovernmental organisations (IGOs) play a pivotal role in this process by advocating for policy reforms, promoting best practices, and facilitating the exchange of knowledge and resources. Through research, reports, and conferences, IGOs help shape the global response to financial crimes, ensuring that countries are equipped with the tools and strategies needed to combat these threats effectively.

Key organisations like the Financial Action Task Force (FATF) and the United Nations Office on Drugs and Crime (UNODC)<sup>51</sup> are at the forefront of these efforts. They raise awareness about emerging risks, share insights on effective strategies, and foster dialogue among policymakers, practitioners, and stakeholders. For example, the FATF sets international standards for anti-money laundering (AML) and counter-terrorist financing (CFT), while the UNODC provides technical assistance and supports the implementation of global treaties. These efforts are complemented by multilateral agreements such as the United Nations Convention against Transnational Organised Crime (UNTOC) and its protocols, which provide a legal framework for countries to collaborate in combating organised crime, including money laundering and terrorist financing.

---

<sup>51</sup> United Nations Convention against Transnational Organised Crime (UNTOC) - Also known as the Palermo Convention, this treaty provides a comprehensive framework for international cooperation in combating organised crime, including money laundering and terrorist financing retrieved from <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> accessed 20 June 2025

In addition to setting standards and monitoring compliance, IGOs play a critical role in capacity building. They help countries develop the expertise and infrastructure needed to implement effective AML/CFT measures. By facilitating information sharing and promoting innovative approaches, these organisations contribute to the adoption of evidence-based policies that address the evolving nature of financial crimes.<sup>52</sup>

In summary, intergovernmental organisations and multilateral agreements are indispensable in the global fight against financial crimes. They set international standards, monitor compliance, facilitate cooperation, and advocate for policy reforms. By fostering collaboration among member states, these organisations help build robust and sustainable AML/CFT regimes, ultimately strengthening the integrity and stability of the global financial system.<sup>53</sup>

The Joint International Task Force on Money Laundering (JITF-AML) is a collaboration of financial intelligence units (FIUs) from many nations to combat money laundering and terrorism funding. Member FIUs collaborate on financial intelligence, conduct joint investigations, and coordinate enforcement operations to disrupt illicit financial flows and dismantle criminal networks.<sup>54</sup> One significant case study that demonstrated the success of international collaboration in combating financial crimes and terrorist financing is Operation Trojan Shield. This was a global law enforcement operation coordinated by the Federal Bureau of Investigation (FBI), the Australian Federal Police (AFP), and the European Union Agency for Law Enforcement Cooperation (Europol). The operation employed encrypted communication networks to target criminal groups involved in drug trafficking, money laundering, and other illegal acts. Law enforcement agencies from more than 16 countries collaborated to infiltrate criminal networks,

---

<sup>52</sup> Ibid

<sup>53</sup> Financial Action Task Force (FATF ). (2022). FATF Mutual Evaluations. Retrieved from <<https://www.fatf-gafi.org/mutual-evaluations/>> Accessed 6 June 2025

<sup>54</sup> networks.

gather evidence, and make arrests, resulting in the seizure of millions of dollars in cash, drugs, and property.<sup>55</sup>.

The Global Magnitsky Act<sup>56</sup> Enables countries to impose targeted sanctions on individuals and entities involved in serious human rights abuses, corruption, and financial crimes. Several countries, including the United States, Canada, and the United Kingdom, have enacted legislation based on the Global Magnitsky Act, allowing for the freezing of assets and travel bans on human rights violators and corrupt officials. Multilateral coordination among countries implementing the Global Magnitsky Act sanctions enhances the impact of targeted measures and promotes accountability for perpetrators of financial crimes and human rights abuses. These case studies demonstrate the effectiveness of international cooperation in combating financial crimes and terrorist financing. By pooling resources, sharing intelligence, and coordinating enforcement actions, countries can disrupt criminal networks, dismantle illicit financial infrastructure, and safeguard the integrity of the global financial system.

### **1.11 Technological Advancement and Innovation**

Technological innovation has transformed the global landscape of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) by equipping financial institutions and law enforcement agencies with more

---

<sup>55</sup> Joint International Task Force on Money Laundering (JITF-AML). (2022). About JITF-AML. Retrieved from <<http://www.jitfaml.org/>> Accessed 23 July 2025

<sup>56</sup> The Global Magnitsky Act is a U.S. law that allows the government to impose targeted sanctions such as asset freezes and travel bans on individuals and entities involved in serious human rights abuses or significant corruption anywhere in the world. Named after Sergei Magnitsky, a Russian lawyer who uncovered a massive tax fraud scheme and died in a Moscow prison after being tortured and denied medical care, the act serves as a tool to hold perpetrators of human rights violations and corrupt actors accountable. However, its effectiveness depends on consistent and impartial application, as well as international cooperation to ensure that perpetrators cannot evade sanctions by moving assets or operating in less regulated jurisdictions. Critics argue that the act is sometimes applied inconsistently, with geopolitical considerations influencing decisions.

sophisticated tools for detection, analysis, and enforcement. Key technological enablers in this context include artificial intelligence (AI), machine learning (ML), big data analytics, and blockchain technology. These innovations have significantly enhanced the precision, speed, and scope of anti-financial crime operations.

### **1.11.1 Advanced Data Analytics and Machine Learning**

AI and ML algorithms enable organisations to analyse vast datasets in real-time, identifying complex patterns, correlations, and anomalous behaviour that may signal financial crime.<sup>57</sup> Traditional rule-based transaction monitoring systems often generate large volumes of false positives; however, advanced data analytics reduce these false alerts by adapting dynamically to evolving criminal tactics.<sup>58</sup> Financial institutions now employ predictive modelling and natural language processing (NLP) to detect suspicious transactions, unusual customer behaviour, and potential shell company structures with far greater accuracy.

### **1.11.2 Real-Time Transaction Monitoring and Proactive Risk Management**

Modern automated transaction monitoring systems, powered by AI, facilitate near-instantaneous screening of customer transactions, allowing institutions to flag high-risk activities in real time. This enables proactive risk management, where threats are neutralised before they escalate.<sup>59</sup> The ability to act quickly on suspicious transactions, especially across borders, is essential in the current era of fast-moving digital payments and crypto-assets.

---

<sup>57</sup> FATF & OECD, Opportunities and Challenges of New Technologies for AML/CFT (2021), available at: <https://www.fatf-gafi.org/publications>.

<sup>58</sup> Basel Institute on Governance, Artificial Intelligence in Anti-Money Laundering Compliance, (2023), available at: <https://www.baselgovernance.org>.

<sup>59</sup> European Banking Authority (EBA), Machine Learning in Anti-Money Laundering – Regulatory Expectations and Market Developments, (2022), available at: <https://www.eba.europa.eu>.

By leveraging these technological advancements, financial institutions not only ensure regulatory compliance but also contribute significantly to the early detection and prevention of complex financial crimes, including cyber-fraud, tax evasion, terrorist financing, and money laundering through virtual assets.

Blockchain research tools enable investigators to track the transfer of funds across cryptocurrency networks, revealing information about unlawful activities such as money laundering and terrorism financing. Law enforcement authorities can use blockchain transactions to identify addresses connected with criminal actors, follow illicit fund transfers, and destroy illicit financial networks operating in the digital arena.<sup>60</sup>

Regulatory technology (RegTech) solutions help financial institutions automate compliance operations and improve their regulatory reporting capabilities. RegTech platforms use technology, including artificial intelligence (AI), natural language processing (NLP), and robotic process automation (RPA), to simplify AML/CFT compliance, enhance risk assessment accuracy, and lower compliance costs. These technologies help financial institutions meet regulatory obligations more effectively while also improving their ability to detect and prevent financial crime.<sup>61</sup>

Open-source intelligence (OSINT) services collect and analyse publicly available data from online sources, social media platforms, and public records to detect potential financial crimes and criminal actions. OSINT tools help law enforcement and financial institutions collect intelligence, conduct investigations,

---

<sup>60</sup> M. Kaur & R. Jain. (2021). Blockchain and Artificial Intelligence: A New Hope for Anti-Money Laundering (AML) Compliance. *International Journal of Financial Management and Economics*, 4(2), pp. 23-29.

<sup>61</sup> S. Kshetri. (2021). How Blockchain, AI, and Other Technologies Could Reinforce AML Compliance. *Journal of Money Laundering Control*, 24(1), pp. 27-39.



and assess risk factors connected with customers, counterparties, and transactions<sup>62</sup>.

Cybersecurity solutions protect financial institutions, and critical Digital identity verification solutions use biometric authentication, document verification, and identity verification services to verify clients' identities and reduce the risk of identity fraud and account takeovers. By adding digital identity verification into customer onboarding processes, financial institutions can improve KYC/AML procedures, strengthen customer due diligence, and lower the risk of illicit activities. Cryptocurrency tracking technologies allow law enforcement and compliance professionals to monitor and analyse cryptocurrency transactions. These tools allow for the discovery of suspicious patterns, the tracking of illicit cash, and the mapping of Bitcoin transfers throughout blockchain networks. Investigators can improve their abilities to combat online money laundering, cybercrime, and terrorism financing by utilising Bitcoin tracking techniques.

Infrastructure from cyber threats, data breaches, and cyberattacks. Organisations can safeguard sensitive data, prevent unauthorised access to financial systems, and lower the risk of cybercrime, including phishing, malware, and ransomware attacks. AI-powered algorithms analyse publicly available data, such as social media profiles and online forums, to gather additional information about customers and assess their risk profile. By integrating blockchain analytics and AI into CDD processes, financial institutions can enhance their understanding of customer behaviour, detect potential red flags, and prevent the on boarding of high-risk customers involved in illicit activities.

These technical breakthroughs and technologies enable financial institutions, regulators, and law enforcement agencies to better tackle financial crime and terrorist financing in an increasingly digitised and linked world. By leveraging

---

<sup>62</sup> Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) available at <https://www.europol.europa.eu/> accessed 23 May 2025

technology, stakeholders can strengthen their capacities and resilience and stay ahead of new challenges in the battle against illicit money. These technologies enable real-time monitoring, predictive analytics, and enhanced risk assessment, empowering stakeholders to combat money laundering, fraud, and terrorist financing in an increasingly digital and interconnected world. AI-powered algorithms analyse publicly available data, such as social media profiles and online forums, to gather additional information about customers and assess their risk profile.<sup>63</sup>

### **1.12 Behavioural Analysis and Anomaly Detection:**

AI algorithms perform behavioural analysis and anomaly detection to identify suspicious patterns and deviations from normal transactional behaviour. By analysing transactional data in real-time, AI-powered systems can detect unusual patterns, such as sudden spikes in transaction volume or unusual transaction flows, which may indicate money laundering or other illicit activities. Behavioural analysis and anomaly detection techniques enable financial institutions to detect emerging threats, adapt to evolving tactics used by criminals, and mitigate risks promptly.<sup>64</sup>

AI-driven predictive analytics use historical data to forecast future trends and predict potential risks associated with blockchain transactions. Machine learning models analyse large datasets to identify risk factors, predict emerging threats, and anticipate changes in the financial crime landscape. Predictive analytics enable financial institutions to proactively identify and address vulnerabilities,

---

<sup>63</sup> Zhang, K. Zhou, X. Wang, & X. Feng. (2021). Research on the Application of AI and Blockchain in Anti-Money Laundering. 2021 3rd International Conference on Information Technology and Artificial Intelligence (ICITAI), Hangzhou, China, pp. 128-132.

<sup>64</sup> Bello Oluwabusayo and Komolafe Olufemi (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges and opportunities. Retrieved from [https://www.researchgate.net/publication/383264952\\_Artificial\\_intelligence\\_in\\_fraud\\_prevention\\_Exploring\\_techniques\\_and\\_applications\\_challenges\\_and\\_opportunities](https://www.researchgate.net/publication/383264952_Artificial_intelligence_in_fraud_prevention_Exploring_techniques_and_applications_challenges_and_opportunities) Retrieved 28 July 2025

strengthen their AML frameworks, and stay ahead of evolving risks posed by financial crimes. By integrating blockchain analytics and AI technologies into AML efforts, financial institutions and regulatory agencies can enhance their ability to detect, investigate, and prevent financial crimes effectively.<sup>65</sup> These technologies enable real-time monitoring, predictive analytics, and enhanced risk assessment, empowering stakeholders to combat money laundering, fraud, and terrorist financing in an increasingly digital and interconnected world.<sup>66</sup>

### **1.13 Conclusion**

The fight against financial crimes and terrorist financing is evolving rapidly, driven by advances in technology, emerging threats, and shifting regulatory landscapes. Tools such as artificial intelligence, machine learning, and blockchain analytics have the potential to revolutionise anti-money laundering (AML) efforts—but they also introduce new complexities, from data privacy concerns to high implementation costs. While financial institutions work to balance compliance, efficiency, and customer experience, global cooperation remains vital. Yet, cross-border data sharing is still hindered by legal and regulatory constraints. The rise of virtual assets and decentralised finance (DeFi) adds another layer of risk, demanding innovative, forward-looking regulatory responses.

Public-private partnerships (PPPs) are key to building trust, enhancing intelligence sharing, and promoting effective enforcement. However, success will depend on overcoming legal, institutional, and governance hurdles. Promoting financial inclusion while ensuring consumer protection must also remain a priority, particularly through the smart application of technology in KYC and AML processes. Finally, the future of AML lies in a collaborative, technology-

---

<sup>65</sup> Ibid

<sup>66</sup>M. Kaur and R. Jain, Blockchain and Artificial Intelligence: A New Hope for Anti-Money Laundering (AML) Compliance(2021). *International Journal of Financial Management and Economics*, 4(2), pp. 23-29.

enabled, and risk-sensitive approach—one that unites stakeholders across sectors and borders to address threats while protecting the integrity of the global financial system.

### **1.14 Findings**

This research reveals several critical challenges undermining the effectiveness of existing Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regimes.

Firstly, there is a persistent lack of effective cross-border coordination, which hampers the detection and disruption of international financial crime networks. Secondly, many national frameworks rely on outdated enforcement tools and are ill-equipped to manage complex, tech-driven threats such as cryptocurrency laundering and cyber-enabled fraud.

Additionally, the paper finds that geopolitical tensions and mistrust between jurisdictions significantly limit international cooperation, impeding the free flow of critical financial intelligence and enabling illicit actors to exploit regulatory gaps.<sup>3</sup> Resource constraints and institutional weaknesses in some regions also limit the capacity of regulators to keep pace with emerging threats. Moreover, the paper also observed that AML legislation in many countries is not regularly reviewed or updated in line with global best practices or FATF Recommendations, leaving legal systems vulnerable to exploitation. These shortcomings collectively undermine global efforts to combat money laundering and terrorist financing.

### **1.15 Recommendations**

To address the above challenges, the paper recommends the following:

1. Strengthening global AML cooperation through binding multilateral treaties, joint enforcement operations, and enhanced information sharing frameworks.

2. Investing in advanced surveillance technologies, including blockchain analytics, artificial intelligence (AI), and machine learning (ML), to improve proactive detection and predictive risk modelling.
3. Building institutional capacity in under-resourced jurisdictions through targeted funding, regulatory training, and technical assistance.
4. Regularly reviewing and updating AML/CTF laws to reflect evolving financial crime risks, emerging technologies, and FATF standards.

Findings reveal that AML frameworks often lack adequate cross-border coordination, suffer from outdated enforcement mechanisms, and are not sufficiently equipped to tackle technologically-enabled financial crimes.<sup>3</sup> Furthermore, current geopolitical tensions have hampered trust, reduced data sharing, and created safe havens for illicit financial flows.<sup>4</sup> In response, the paper recommends

In conclusion, the paper argues that without comprehensive legal reform, stronger international partnerships, and the integration of technology-driven solutions, the fight against money laundering and terrorist financing will remain insufficient. A coordinated and adaptive AML regime is thus essential for preserving financial transparency, economic resilience, and global security.