INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 3 | 2025 Art. 31

Cross-Border Challenges in Digital AML Compliance: A Legal and Technological Perspective

Sunny Kumar
LL.M Student,
University School of Law, Rayat Bahra University

Priyanka Dhiman
Assistant Professor,
University School of Law, Rayat Bahra University

Recommended Citation
Sunny Kumar and Priyanka Dhiman, *Cross-Border Challenges in Digital AML Compliance: A Legal and Technological Perspective*, 4 IJHRLR 486-498 (2025).
Available at www.humanrightlawreview.in/archives/.

Cross-Border Challenges in Digital AML Compliance: A Legal and Technological Perspective

Sunny Kumar
LL.M Student,
University School of Law, Rayat Bahra University

Priyanka Dhiman
Assistant Professor,
University School of Law, Rayat Bahra University

Manuscript Received	Manuscript Accepted	Manuscript Published
18 May 2025	23 May 2025	27 May. 2025

ABSTRACT

The digital transformation of financial services has intensified the complexity of anti-money laundering (AML) compliance, particularly in cross-border contexts. This paper explores the legal and technological challenges involved in enforcing AML standards in an increasingly digitized and globalized financial ecosystem. It identifies key vulnerabilities, including regulatory fragmentation, jurisdictional arbitrage, and the uneven oversight of digital service providers. The paper also examines the potential of technological innovations such as AI-driven monitoring, blockchain analytics, and digital identity verification to strengthen compliance frameworks. However, these technologies face limitations in interoperability, accuracy, and privacy. Emphasis is placed on the need for greater international cooperation through harmonized legal standards, multilateral institutions, and public-private partnerships. The paper concludes by advocating for an integrated approach that balances regulatory consistency, technological advancement, and data protection to develop a resilient global AML regime. This holistic framework is essential to combat modern money laundering schemes that transcend borders and exploit digital loopholes.

KEYWORDS

Anti-money laundering, digital finance, regulatory arbitrage, blockchain analytics, cross-border compliance, financial crime, RegTech.

INTRODUCTION: A NEW BATTLEFIELD AGAINST FINANCIAL CRIME

"Criminals go where the money is, and increasingly, that means going digital."[1]

As digital finance rapidly transcends borders, money laundering operations have evolved in both scale and complexity. The financial environment of today, which is molded by cryptocurrencies, fast transaction systems, and cross-border fintech platforms, offers authorities both enormous opportunities and difficult obstacles. Policymakers, law enforcement, and financial institutions all have serious concerns about cross-border AML compliance because globalization and digitization have surpassed traditional AML standards.

Money can move between countries in a matter of seconds thanks to the increased interconnectedness of the global financial system. Even though financial technology has developed quickly, worldwide anti-money laundering (AML) regulations are still disjointed, which gives money launderers the opportunity to take advantage of legal gaps and regulatory arbitrage. Cooperation between countries is further complicated by national sovereignty, disparate data privacy laws, and uneven enforcement standards.

In the context of AML compliance, this study aims to investigate the technological and regulatory difficulties presented by cross-border digital financial transactions. It also looks into how contemporary technologies, such blockchain analytics, artificial intelligence (AI), and RegTech, might improve compliance systems. This study intends to suggest workable legislative and technological solutions to stop money laundering globally by pointing out places for harmonization and innovation as well as the gaps in the current regulatory frameworks.

THE RISE OF CROSS-BORDER DIGITAL FINANCIAL ECOSYSTEMS

Due to the digitization of financial services, a new era of ease, accessibility, and worldwide connectivity has begun. The manner that money is saved, moved, and invested has been completely transformed by fintech companies, cryptocurrency platforms, neobanks, and cross-border payment gateways. However, this quick innovation has also made it harder to detect and stop money laundering because it has increased the channels for illegal

[1] Europol. (2021). *Internet Organised Crime Threat Assessment*. Retrieved from https://www.europol.europa.eu.

financial transfers.

1. **Growth of Fintech and Digital Banking Across Borders**

   Cross-border transactions can be completed almost instantly with digital banking services like Revolut, PayPal, and Wise (previously TransferWise). These organizations operate across several jurisdictions without constant regulatory inspection, have little physical presence, and frequently conduct customer onboarding remotely. It is difficult for national AML authorities to keep an eye on operations in real time because of this decentralization.

2. **The Role of Cryptocurrencies and Decentralized Finance (DeFi)**

   Since they are anonymous or pseudonymous, cryptocurrencies—particularly privacy-focused ones like Monero and Zcash—present distinct AML issues. DeFi platforms further obfuscate the source and destination of payments by enabling peer-to-peer transactions without the need for middlemen. According to blockchain analytics company Chainalysis, over $20 billion worth of illicit cryptocurrency transactions occurred in 2022 alone, with DeFi protocols and mixers accounting for a large portion of these transactions.[2]

3. **Velocity and Volume of Transactions**

   Digital platforms provide quick, large-scale transactions that can be divided into smaller sums (a strategy called smurfing) to evade discovery. Traditional rule-based monitoring systems are overwhelmed by the volume and speed of digital transactions, which makes it more difficult to identify suspicious activity, particularly when it occurs internationally.

In essence, although digital financial systems promote efficiency and inclusivity, they also introduce weak spots into the worldwide AML framework. Maintaining compliance technology and regulatory frameworks in line with these rapid advancements is a challenge.

LEGAL FRAMEWORKS AND JURISDICTIONAL CONFLICTS

The fragmentation of legal regimes is one of the main obstacles to cross-border AML compliance. AML legislation, enforcement priorities, and classifications of suspicious conduct are specific to

[2] Chainalysis. (2023). *The 2023 Crypto Crime Report*. Retrieved from https://www.chainalysis.com.

each nation or region. These discrepancies impede efficient enforcement and provide openings for criminals to take advantage of in a digital economy where financial transactions are readily transnational.

1. **Divergent National Regulations**

   While worldwide guidelines established by the Financial Action Task Force (FATF) serve as a baseline, how AML obligations—such as customer due diligence, reporting limits, and penalties—are carried out varies greatly. While the European Union implements rigorous anti-money laundering directives across member states, territories such as the British Virgin Islands and Seychelles have more liberal regimes. This creates safe havens for illegal fund transfers and money laundering operations.

2. **Limitations in Mutual Legal Assistance Treaties (MLATs)**

   Although MLATs are essential tools for international collaboration in criminal investigations, they are frequently cumbersome, inefficient, and unsuitable for the rapid pace of financial crime committed online. Information requests between nations might take months, and by then, the trail might have been abandoned. Furthermore, there are gaps in the investigatory reach because not all nations have MLATs with one another.

3. **Case Study: India, the EU, and the United States**

   The Prevention of Money Laundering Act (PMLA) governs AML compliance in India, whereas the Bank Secrecy Act (BSA) and the PATRIOT Act are enforced in the United States. The AML Directives are unique to the EU. Standards for crypto service providers, beneficial ownership disclosure, and reporting suspicious behavior vary by jurisdiction. It takes a lot of resources and legal expertise for multinational fintech companies doing business in these areas to concurrently comply with all relevant laws.

4. **Data Privacy vs. AML Obligations**

   AML compliance requirements that include the gathering and exchange of consumer data may conflict with the General Data Protection Regulation (GDPR) of the European Union. Similar conflicts arise in other places where cross-border data flow is restricted by privacy rules, making it more difficult to keep an eye on suspicious conduct in real time.

Regulatory arbitrage, in which money launderers deliberately transfer assets between nations with laxer regulations, is encouraged by the absence of a uniform legal framework throughout jurisdictions. Any significant advancement in cross-border AML enforcement must address these jurisdictional disparities.

REGULATORY ARBITRAGE AND GAPS IN COMPLIANCE

A major consequence of diverse AML regimes is the growth of regulatory arbitrage—a method used by money launderers to shift illicit cash with minimum detection risk by exploiting weaker or conflicting restrictions across nations. This approach is especially common in the digital banking environment, where the physical locations of users, servers, and institutions frequently blur traditional regulatory lines.

1. Exploiting Weak Jurisdictions

Individuals involved in money laundering frequently focus on nations that have weak anti-money laundering (AML) regulations, insufficient financial oversight, or strict confidentiality practices. These "non-cooperative countries," as regularly noted by the Financial Action Task Force (FATF), serve as channels for illegal transactions. A common money laundering path might start in a jurisdiction with minimal know-your-customer (KYC) standards, transit through intermediaries operating on loosely regulated digital platforms, and ultimately reach a highly regulated nation where the funds seem to be legitimate.

2. Gaps in Licensing and Oversight of Digital Service Providers

Digital payment platforms, cryptocurrency exchanges, and wallet services face varying levels of regulation depending on the country. In certain regions, they can function without licenses or anti-money laundering (AML) requirements, which can facilitate the hiding of fund origins. This gap in regulation continues to exist despite the FATF's “Travel Rule” introduced in 2019, which requires virtual asset service providers to exchange identifying details during transactions.

3. Compliance Fatigue in Multinational Institutions

Large financial institutions operating across multiple regions face difficulties in maintaining a consistent AML compliance program. Differing reporting standards, thresholds for suspicious transactions, and customer identification

requirements make it costly and complicated to comply with every applicable law. In response, some institutions prioritize compliance in stricter jurisdictions while relaxing standards elsewhere, thereby creating systemic vulnerabilities.

4. Case Example: Binance and Jurisdictional Avoidance

The world's largest crypto exchange, Binance, has faced repeated criticism for its opaque corporate structure and avoidance of regulatory scrutiny. By not maintaining a clear headquarters and operating in multiple countries with varying degrees of oversight, Binance was able to delay regulatory compliance in several jurisdictions until investigations and penalties forced a change.[3]

Addressing these regulatory weaknesses necessitates not only domestic reforms but also international collaboration, unified compliance frameworks, and protocols for real-time information sharing. In the absence of this integration, the global financial system continues to be vulnerable to exploitation by increasingly advanced money laundering networks.

TECHNOLOGICAL TOOLS AND THEIR ROLE IN AML COMPLIANCE

As conventional AML systems find it difficult to keep up with the rapid growth and volume of digital transactions, technology has become both essential and a chance to combat cross-border money laundering. Innovative solutions, ranging from sophisticated analytics to blockchain tracing, provide scalable methods for identifying suspicious activity—but they also come with their own set of challenges.

1. RegTech and AI-Driven Monitoring Systems

Regulatory Technology (RegTech) encompasses solutions that utilize artificial intelligence (AI), machine learning, and big data analytics to support regulatory compliance efforts. In the realm of Anti-Money Laundering (AML), these technologies process large amounts of transaction data to identify irregularities, create alerts, and evaluate customer risk profiles in real-time. For instance, AI can identify sophisticated layering methods or analyze user behavior in relation to established money laundering typologies.

[3] Financial Times. (2023). *Binance's regulatory struggles spotlight compliance risks in crypto*. Retrieved from https://www.ft.com

2. Blockchain Analytics and KYT (Know Your Transaction)

The inherent transparency of blockchain facilitates the utilization of instruments such as Chainalysis, Elliptic, and CipherTrace to monitor the movement of cryptocurrency between wallets and exchanges. In contrast to conventional KYC (Know Your Customer), KYT emphasizes the observation of transaction behavior itself—including frequency, source, and destination patterns—thereby allowing for the timely identification of illicit transfers.

3. Opportunities in Digital Identity Verification

Technologies including biometric KYC, digital ID systems, and eKYC diminish identity fraud during remote onboarding procedures. Cross-border efforts such as the EU's eIDAS (electronic Identification and Trust Services) regulation seek to create interoperable digital identities to improve AML compliance throughout the area.

4. Limitations and Ethical Dilemmas

Despite their promise, technology-driven AML systems face limitations:

- **False positives**: AI-based systems may trigger excessive alerts, overwhelming compliance teams.
- **Interoperability issues**: Different systems and standards in various jurisdictions complicate real-time coordination.
- **Data privacy**: Automated surveillance can infringe on privacy rights, especially under stringent regulations like GDPR.

Furthermore, offenders are progressively utilizing technology for their own purposes—employing AI-created identities, mixers, and anonymization tools—to evade detection. Thus, technology needs to continuously advance, and regulators have to guarantee that technological implementation is in accordance with legal requirements and ethical standards.

Although technology has the potential to enhance AML capabilities, it is not a cure-all. It needs to be integrated within a well-organized legal and institutional framework to unlock its complete potential.

INTERNATIONAL COOPERATION AND POLICY INITIATIVES

Due to the inherently transnational character of digital money laundering, no individual nation can effectively tackle it alone.

Collaborative efforts on international levels—legal, operational, and technological—are essential to bridging jurisdictional gaps and making sure that AML enforcement evolves alongside emerging threats. Numerous multilateral organizations and initiatives have been striving for this goal, yet obstacles still exist.

1. **The Role of the Financial Action Task Force (FATF)**

   FATF establishes worldwide AML standards and observes member nations for adherence through mutual assessments. Its "grey" and "black" lists exert pressure on regions with systemic shortcomings. FATF has additionally broadened its standards to cover virtual assets and Virtual Asset Service Providers (VASPs) via the "Travel Rule. " Nonetheless, the execution of these guidelines differs markedly among nations, diminishing their overall efficacy.

2. **Egmont Group and Financial Intelligence Units (FIUs)**

   The Egmont Group promotes the global exchange of information among FIUs, enabling faster sharing of suspicious transaction data across borders. Though this serves as a useful resource, involvement is optional, and certain nations may not have the necessary infrastructure or political motivation to participate actively.

3. **Public-Private Partnerships (PPPs)**

   Collaborative frameworks like the United Kingdom's Joint Money Laundering Intelligence Taskforce (JMLIT) and the U. S. FinCEN Exchange have showcased the importance of immediate cooperation between government bodies and financial organizations. These programs enhance the sharing of information and the identification of threats while minimizing the repetition of work.

4. **Regional Efforts and Bilateral Agreements**

   AML Directives (AMLD) have been implemented by the European Union, with the aim of creating a centralised EU ALM. At the same time, nations such as India have formed bilateral agreements with financial regulators in different countries to aid in investigations. Nevertheless, coordination remains inconsistent, and jurisdictional sovereignty continues to restrict the extent of collaboration.

5. **Need for Unified Digital Standards**

   A significant barrier to effective international AML enforcement

is the lack of unified digital identity and transaction monitoring standards. Interoperable systems for e-KYC, cross-border reporting, and data exchange could greatly enhance efficiency, but necessitate political consensus and standardization across legal frameworks.

Over the past decade, there has been progress in international cooperation, but difficulties with electronic commerce and legal systems, as well as issues with data protection, persist. The subsequent phase must focus on not only aligning regulations but also creating global digital infrastructures for AML compliance.

WAY FORWARD: BRIDGING LEGAL AND TECHNOLOGICAL GAPS

To enhance cross-border AML compliance in the digital era, it is crucial to align legal frameworks with technological progress. This process starts with harmonizing international laws. While the FATF sets forth global guidelines, their successful execution relies on the commitment of individual nations. Countries need to implement uniform definitions of money laundering, set compatible reporting thresholds, and establish clear regulatory standards for new technologies like cryptocurrencies and digital identity verification. Legal frameworks should also enable quick adaptations to changing typologies, allowing regulators to respond swiftly to emerging threats.

In conjunction with legal reforms, investing in strong technological infrastructures is vital. Governments and financial institutions ought to utilize advanced analytics, AI-driven monitoring tools, and blockchain intelligence solutions that facilitate real-time identification of suspicious transactions across borders. These tools should be interoperable and constructed to function across different jurisdictions. The creation of regional or global shared platforms for monitoring suspicious transactions—managed by neutral entities or multilateral institutions—could greatly enhance transparency and responsiveness.

Moreover, improving digital identity systems is a critical initial step toward enhancing cross-border compliance. The creation of secure, interoperable e-KYC protocols, supported by biometric verification and blockchain-based identity records, would allow for more precise customer due diligence without compromising data integrity. Governments should also encourage public-private partnerships that unite regulatory agencies, financial institutions, and technology providers to collaboratively design and test AML solutions within regulatory sandboxes.

Nevertheless, these initiatives must be balanced with the need for privacy protections and accountability. Technological surveillance in AML should not infringe on civil liberties. Therefore, it is crucial to establish oversight mechanisms to ensure that data usage adheres to human rights standards and data protection laws such as GDPR. Cross-border data sharing protocols should incorporate strong encryption, clauses for purpose limitation, and safeguards for data retention.

Closing the divide between law and technology in AML compliance is not merely about efficiency—it is essential for protecting the global financial system. A coordinated, multi-stakeholder approach that fuses legislative consistency, technological advancement, and ethical governance is necessary for establishing a robust and future-ready AML framework.

CONCLUSION: TOWARD A COHESIVE GLOBAL RESPONSE

The transformation of finance through digital means has resulted in significant advantages regarding accessibility, efficiency, and innovation—but it has also created serious vulnerabilities in the global struggle against money laundering. In the context of cross-border transactions, these vulnerabilities are intensified by disjointed legal systems, variable enforcement, and shortcomings in technological adoption. As money launderers become increasingly sophisticated and digital ecosystems grow more intricate, the shortcomings of conventional AML frameworks become clearer.

This paper has examined how legal disunity, jurisdictional exploitation, and the inadequacy of outdated compliance models impede effective AML enforcement across borders. It has also underscored the potential of emerging technologies—like RegTech, blockchain analytics, and AI—in improving monitoring, due diligence, and reporting capabilities. However, technology by itself cannot address the issue; it must be integrated into cohesive legal and regulatory frameworks, bolstered by strong international cooperation.

Looking ahead, stakeholders need to implement a comprehensive and coordinated approach that unifies law, policy, and innovation. This involves aligning AML regulations, constructing interoperable digital infrastructures, and encouraging cross-border cooperation through both formal agreements and informal partnerships. Equally crucial is the necessity to safeguard individual rights and uphold ethical standards in the use of surveillance technologies.

In a landscape where illicit money moves instantaneously,

global AML initiatives must also be swift, intelligent, and integrated. Only then can we aspire to build a secure, transparent, and equitable financial system that keeps pace with the digital age.

REFERENCES

1. Chainalysis. (2023). *The 2023 Crypto Crime Report*. Retrieved from https://www.chainalysis.com

2. Financial Action Task Force (FATF). (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Retrieved from https://www.fatf gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

3. Financial Action Task Force (FATF). (2022). *High-Risk Jurisdictions subject to a Call for Action – February 2022*. Retrieved from https://www.fatf-gafi.org

4. Financial Times. (2023, March). *Binance's regulatory struggles spotlight compliance risks in crypto*. Retrieved from https://www.ft.com

5. Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from https://www.europol.europa.eu

6. Egmont Group. (n.d.). *About the Egmont Group*. Retrieved from https://egmontgroup.org/en/content/about

7. European Commission. (2021). *Anti-money laundering and countering the financing of terrorism legislative package*. Retrieved from https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en

8. JMLIT. (2022). *The Joint Money Laundering Intelligence Taskforce Annual Report*. UK Home Office. Retrieved from https://www.gov.uk/government/publications/joint-money-laundering-intelligence-taskforce-annual-report

9. U.S. Department of the Treasury. (2021). *Anti-Money Laundering Act of 2020 – Key Provisions*. Retrieved from https://home.treasury.gov

10. CipherTrace. (2021). *Cryptocurrency Crime and Anti-Money Laundering Report*. Retrieved from https://ciphertrace.com/cryptocurrency-anti-money-laundering-report-2021/

11. Elliptic. (2022). *Crypto Compliance and Blockchain Analytics*. Retrieved from https://www.elliptic.co

12. FATF. (2021). *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs*. Retrieved from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets.html

13. OECD. (2022). *Tax and Crime: Digital Disruption and Money Laundering*. Retrieved from https://www.oecd.org

14. World Bank. (2020). *Enhancing Financial Integrity: Policies to Combat Money Laundering*. Retrieved from https://www.worldbank.org

15. KPMG. (2022). *Emerging AML Technologies and Regulatory Trends*. Retrieved from https://home.kpmg