BEYOND THE PAPER TRAIL

Digital Hawala and the Enforcement Gaps in India's Anti-Money Laundering Regime

by

Anushka Acharya & Manushree MB

ABSTRACT

The rapid digitalisation of financial systems has transformed illicit financial transactions, enabling traditional hawala networks to operate through online banking, fintech platforms, virtual digital assets, and encrypted communication technologies. While these innovations improve financial accessibility, they also complicate the detection and prosecution of money laundering offences. The Prevention of Money Laundering Act, 2002 (PMLA) is India's primary anti-money laundering legislation; however, its effectiveness in addressing technology-enabled hawala networks remains a challenge. This paper adopts a doctrinal and comparative approach to evaluate the adequacy of the PMLA by examining its statutory framework, the enforcement role of the Enforcement Directorate (ED) and the Financial Intelligence Unit-India (FIU-IND), judicial developments, and reporting obligations. Drawing on the Financial Action Task Force (FATF) Recommendations and international anti-money laundering frameworks, the paper identifies regulatory gaps and advocates technology-driven reforms, including AI-enabled financial intelligence, stronger compliance measures, enhanced inter-agency coordination, and improved cross-border cooperation. It concludes that modernising India's anti-money laundering framework is essential to effectively combat digital hawala while balancing financial innovation, regulatory efficiency, and due process.

Keywords: *Digital Hawala; Prevention of Money Laundering Act, 2002 (PMLA); Money Laundering; Financial Intelligence Unit (FIU-IND); Enforcement Directorate (ED); Anti-Money Laundering (AML); Financial Action Task Force (FATF); Digital Economy; Financial Crime.*

I. Introduction

Hawala is a centuries-old, trust-based system of value transfer that moves funds across jurisdictions without the physical or electronic movement of money through the formal banking channel. A remitter pays a local hawaladar, who instructs a counterpart in the destination jurisdiction to pay the beneficiary; the two hawaladars settle their mutual obligations later, often through trade invoicing, counter-remittances, or informal netting. Because the system leaves no conventional audit trail and relies on kinship and community networks rather than documentation, it has long been recognised as a vector for money laundering, terrorist financing, and capital flight.

The last decade has witnessed a structural transformation of this informal value transfer system. Hawaladars no longer depend solely on physical ledgers, couriers, or word-of-mouth networks; they increasingly use mobile banking applications, Unified Payments Interface (UPI) rails, prepaid instruments, shell e-commerce transactions, peer-to-peer virtual digital asset (VDA) transfers, and end-to-end encrypted messaging platforms to instruct and settle transactions. This hybridisation, referred to in this paper as 'digital hawala', combines the anonymity and informality of the traditional hawala network with the speed, scale, and jurisdictional reach of digital finance. It thereby erodes the practical utility of conventional anti-money laundering (AML) tools, which were designed primarily around bank-mediated, geographically anchored transactions.

India's principal legislative response to money laundering, the Prevention of Money Laundering Act, 2002 (PMLA), was enacted to give effect to India's obligations under international conventions and FATF standards, and to enable the tracing, freezing, and confiscation of proceeds of crime. The statute has since been substantially amended, most notably through the Finance Act, 2015, the Finance Act, 2018, the Finance Act, 2019, and the March 2023 notification bringing virtual digital asset service providers within the PMLA's reporting architecture. Enforcement rests principally with the Enforcement Directorate (ED), which investigates the offence of money laundering, and the Financial Intelligence Unit-India (FIU-IND), which receives and analyses suspicious transaction reports (STRs) from reporting entities and disseminates financial intelligence to law enforcement and regulatory agencies.

Commented [1]: This list of amendments omitted the Finance Act, 2018, which is the amendment that reinstated the twin bail conditions under Section 45 after the Supreme Court struck down the earlier version of that section in Nikesh Tarachand Shah v Union of India (2018). This amendment is directly relevant to the discussion of Section 45 later in this paper, so it has been added here to keep the introduction consistent with the rest of the paper. Source: Mondaq, 'Twin Conditions for Bail Under the PMLA' (Mondaq, 7 June 2023).

This paper asks a narrow but consequential question: is the PMLA, as presently designed and enforced, adequate to address hawala networks that have migrated onto digital rails? Adopting a doctrinal method supplemented by comparative analysis, the paper examines the statutory text of the PMLA, the institutional mandates of the ED and FIU-IND, the trajectory of Supreme Court jurisprudence on the Act's constitutional validity and procedural safeguards, and India's standing under the FATF Recommendations following its 2024 Mutual Evaluation. It argues that while India's technical compliance with international AML standards is strong, structural gaps persist in real-time detection, virtual asset tracing, inter-agency data sharing, and cross-border cooperation, each of which digital hawala networks are able to exploit. The paper concludes with a set of reform proposals directed at closing these gaps without diluting the due process protections that Indian courts have increasingly emphasised.

II. Conceptualising Digital Hawala: From Trust-Based Networks to Technology-Enabled Value Transfer

Digital hawala is not a distinct legal category but a descriptive term for the convergence of informal value transfer systems (IVTS) with formal and semi-formal digital financial infrastructure. Four overlapping typologies illustrate this convergence.

A. Fintech-Layered Hawala

Hawaladars increasingly use mobile wallets, UPI handles registered under synthetic or mule identities, and prepaid payment instruments to settle domestic legs of a hawala transaction. The formal digital payment rail is used only for the final-mile transfer, while the cross-border netting between hawaladars continues through informal trade-based settlement, making the digital footprint appear to be an ordinary retail transaction. Empirical evidence suggests that this layering dynamic already operates at considerable scale: financial institutions and cybercrime authorities had flagged more than 2.47 million Layer-1 mule accounts to the Indian Cyber Crime Coordination Centre by early 2026, many of them opened using borrowed or fabricated Know Your Customer credentials before being networked into UPI-linked payment chains.[1] Because each individual mule account typically receives transfers below the reporting threshold that would trigger bank

[1] Business Standard, 'Mule Accounts Decoded: The Hidden Banking Layer Behind Cybercrime' (Business Standard, 25 June 2026) <https://www.business-standard.com/finance/news/what-are-mule-accounts-cybercrime-banking-layer-india-fraud-rbi-126062400855_1.html> accessed 27 August 2026.

scrutiny, it is the aggregation of numerous such accounts into a single settlement chain, rather than any single transaction, that reveals the underlying fintech-layered hawala scheme.

B. Trade-Based and E-Commerce Laundering

Over and under-invoicing of goods, fictitious e-commerce sales, and manipulation of online marketplace escrow and refund mechanisms allow value to move across borders under the guise of commercial activity, without triggering the currency transaction or suspicious transaction thresholds that would ordinarily alert a bank.

C. Virtual Digital Asset (VDA) Hawala

Peer-to-peer transfers of cryptocurrency, stablecoins, and non-fungible tokens (NFTs) allow value to be moved across borders in minutes, using pseudonymous wallet addresses and decentralised or peer-to-peer exchanges that may fall outside the Know Your Customer (KYC) net. Layering through mixers, cross-chain bridges, and non-custodial wallets can sever the audit trail almost entirely, replicating in code what hawaladars historically achieved through personal trust. An illustrative instance of this convergence emerged from the Enforcement Directorate's investigation into the 'E-Nugget' online gaming application, in which proceeds routed through roughly 2,500 mule bank accounts were subsequently layered into wallets held with Binance, ZebPay, and WazirX, allowing the agency to eventually freeze close to Rs 90 crore across the three exchanges.[2] The case illustrates how fiat-to-crypto layering allows illicit proceeds to move through domestic mule-account networks before exiting into virtual asset infrastructure that is comparatively difficult to trace and repatriate.

D. Encrypted-Communication Coordination

Instructions between hawaladars and their counterparts, historically conveyed by courier or coded telephone calls, now travel through end-to-end encrypted applications, sometimes using

[2] Deccan Herald, 'ED Seizes Rs 90 Cr Funds Kept in Binance, ZebPay, WazirX Wallets' (Deccan Herald) <https://www.deccanherald.com/india/ed-seizes-rs-90-cr-funds-kept-in-binance-zebpay-wazirx-wallets-3001695> accessed 27 August 2026.

disappearing messages, which are largely impervious to lawful interception absent platform cooperation.

Each typology retains hawala's defining feature settlement of an obligation without a corresponding cross-border movement of money while inheriting the scale, speed, and jurisdictional dispersion of digital finance. This combination is what renders conventional, transaction-by-transaction AML supervision structurally inadequate: the individual legs of a digital hawala transaction are each designed to look unremarkable, and it is only their aggregation across accounts, wallets, and jurisdictions that reveals the underlying scheme.

III. The Statutory Architecture of the PMLA, 2002

A. The Offence of Money Laundering and 'Proceeds of Crime'

Section 3 of the PMLA defines the offence of money laundering broadly, covering any process or activity connected with the proceeds of crime, including concealment, possession, acquisition, use, or projecting or claiming such proceeds as untainted property. The offence is predicated on a 'scheduled offence' listed in the Schedule to the Act, which spans provisions of the Indian Penal Code (now substantially replaced by the Bharatiya Nyaya Sanhita, 2023), the Narcotic Drugs and Psychotropic Substances Act, 1985, the Unlawful Activities (Prevention) Act, 1967, and numerous economic and regulatory statutes. Because money laundering is a standalone offence dependent on, but not co-extensive with, the predicate offence, the Supreme Court has held that PMLA proceedings can continue independently of the outcome of the predicate prosecution, so long as proceeds of crime are shown to exist. This structure is well suited to hawala transactions linked to identifiable predicate crimes such as drug trafficking or corruption, but is less effective where the predicate offence itself is difficult to establish, as is often the case where hawala is used merely to circumvent foreign exchange controls or tax reporting rather than to launder proceeds of an independently prosecutable crime.

B. Reporting Entities and the 2023 Extension to Virtual Digital Assets

Chapter IV of the PMLA casts reporting, record-keeping, and client due diligence obligations on 'reporting entities', defined under Section 2(1)(wa) to include banking companies, financial institutions, intermediaries, and persons carrying on a 'designated business or profession' under

Section 2(1)(sa). By a notification dated 7 March 2023 issued under Section 2(1)(sa)(vi), the Department of Revenue, Ministry of Finance, brought a wide range of virtual digital asset activities exchange between VDAs and fiat currency, exchange between VDAs, transfer of VDAs, safekeeping or administration of VDAs, and participation in the issuance or sale of VDAs within the definition of designated business, thereby classifying virtual digital asset service providers (VDASPs) as reporting entities. This brought India's regime broadly into line with the FATF's 'Virtual Asset Service Provider' standard and imposed KYC, beneficial ownership verification, and record-retention obligations (for a minimum of five years) on VDASPs. The notification, however, applies only to entities that can be identified and regulated as intermediaries; it does not, and structurally cannot, reach peer-to-peer transfers between self-custodied wallets that never pass through a regulated exchange, nor does it extend to VDASPs operating entirely outside Indian jurisdiction but accessible to Indian users online. India has nonetheless developed an indirect enforcement lever against such offshore platforms: in December 2023, FIU-IND issued compliance show-cause notices under Section 13 of the PMLA to nine offshore virtual digital asset service providers, including Binance and KuCoin, and asked the Ministry of Electronics and Information Technology to block their web and mobile access within India.[3] By late 2025 this compliance mechanism had been extended to twenty-five offshore platforms, with monetary penalties ranging from roughly Rs 34.5 lakh to over Rs 18 crore, and exchanges such as Binance and KuCoin subsequently registered as reporting entities in order to resume Indian operations.[4] This suggests that although the reporting-entity framework cannot compel an offshore VDASP to register, platform-blocking has functioned as a practical, if indirect, substitute for direct regulatory jurisdiction.

C. Attachment, Adjudication, and Confiscation

[3] CoinDesk, 'India to Block URLs of 9 Offshore Exchanges Including Binance After Issuing Compliance "Show Cause" Notices' (CoinDesk, 28 December 2023, updated 8 March 2024) <https://www.coindesk.com/policy/2023/12/28/india-issues-compliance-show-cause-notices-to-9-offshore-exchanges-including-binance-and-kucoin> accessed 27 August 2026.

[4] Cyril Amarchand Mangaldas, 'FIU-IND's Annual Report 2024-25: Trends and Takeaways for India's Digital Assets Industry' (India Corporate Law, 15 January 2026) <https://corporate.cyrilamarchandblogs.com/2026/01/fiu-inds-annual-report-2024-25-trends-and-takeaways-for-indias-digital-assets-industry/> accessed 27 August 2026.

Sections 5 and 8 empower the ED to provisionally attach property believed to be proceeds of crime, subject to confirmation by the Adjudicating Authority and eventual confiscation on conviction, while Section 8(4) permits the ED to take possession of attached property even before trial concludes. This asset-focused architecture is valuable against hawala networks because it allows the State to freeze the fruits of laundering even where the underlying settlement mechanism (informal netting) itself leaves no trace, provided some identifiable and attachable property can be traced to the scheme. The corresponding weakness is that digital hawala, particularly its VDA and offshore variants, can move value into forms and jurisdictions that are difficult to locate, freeze, or repatriate before dissipation.

D. Investigative Powers, the Reverse Burden, and Section 45

Sections 17, 18, and 19 confer search, seizure, and arrest powers on the ED without the ordinary requirement of a First Information Report (FIR); Section 24 places a reverse burden on the accused to prove that alleged proceeds of crime are untainted; and Section 45 imposes 'twin conditions' for bail, requiring the accused to satisfy the court both that there are reasonable grounds to believe the accused is not guilty and that the accused is unlikely to commit any offence while on bail. This combination gives the ED considerable investigative leverage in hawala-linked prosecutions, where direct documentary evidence is often unavailable and circumstantial or intelligence-based evidence predominates. It has also generated sustained constitutional controversy, discussed in Part V below.

IV. Institutional Enforcement: The Enforcement Directorate and FIU-IND

A. The Enforcement Directorate

The ED, functioning under the Department of Revenue, Ministry of Finance, is the principal investigating and prosecuting agency under the PMLA, and also administers the Foreign Exchange Management Act, 1999 (FEMA) and the Fugitive Economic Offenders Act, 2018. Its dual mandate under PMLA and FEMA is particularly relevant to hawala, since unauthorised cross-border remittance frequently implicates both statutes. In digital hawala cases, ED investigations increasingly rely on financial forensics tracing VDA wallet clusters through blockchain analytics tools, correlating UPI and bank transaction patterns, and analysing device and IP metadata obtained from telecom and platform intermediaries rather than the physical ledgers ('parchi' or 'chit' records) that characterised earlier hawala investigations.

B. FIU-IND

FIU-IND, established in 2004 and functioning under the Department of Revenue, is India's central national agency for receiving, processing, analysing, and disseminating information on suspicious financial transactions. Reporting entities are required under Section 12 of the PMLA to furnish Cash Transaction Reports (CTRs), Suspicious Transaction Reports (STRs), and, since the 2023 extension, equivalent reports from VDASPs. FIU-IND is India's representative in the Egmont Group of Financial Intelligence Units, which facilitates the secure international exchange of financial intelligence. Its analytical output feeds both the ED and other law enforcement and regulatory agencies, making it the principal 'upstream' node for the detection of unusual transaction patterns indicative of digital hawala.

C. Coordination Gaps

Notwithstanding a growing body of Memoranda of Understanding between FIU-IND, the ED, the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Central Board of Direct Taxes (CBDT), and state police economic offences wings, the practical reality of inter-agency coordination remains uneven. STRs filed by banks and VDASPs are analysed largely in isolation from telecom-derived intelligence held by law enforcement, and cross-border requests routed through the ED's international cooperation division or through Mutual Legal Assistance Treaties (MLATs) remain slow relative to the speed at which digital value can be moved and dissipated. Because digital hawala transactions are, by design, structured to fall below individually suspicious thresholds and to be dispersed across multiple reporting entities and jurisdictions, effective detection depends on the capacity to correlate data across agencies and borders in near-real time a capability the current architecture only partially supports. The consequences of this fragmentation are visible in enforcement outcomes: of the 911 prosecution complaints filed by the ED between January 2019 and October 2024, only 42 had resulted in a conviction, a rate of approximately 6.42 per cent, with 257 cases still pending trial.[5] A low conviction rate cannot be attributed to coordination failures alone, but it is consistent with the difficulty of converting intelligence-led, multi-agency financial evidence of the kind generated by dispersed digital hawala transactions into evidence capable of sustaining a conviction at trial.

V. Judicial Developments

A. Vijay Madanlal Choudhary v. Union of India (2022)

The constitutional foundations of the PMLA's enforcement architecture were comprehensively tested in *Vijay Madanlal Choudhary v. Union of India*, decided by a three-judge bench of the Supreme Court on 27 July 2022. Rejecting a batch of over two hundred petitions, the Court upheld the constitutional validity of the ED's search, seizure, and arrest powers under Sections 17 and 19; the provisional attachment mechanism under Section 5; the admissibility of statements recorded under Section 50; the reverse burden of proof under Section 24; and the twin conditions for bail under Section 45. The Court characterised money laundering as an offence with grave cross-border and national-security dimensions, a characterisation that has since shaped the weighing of liberty interests against enforcement imperatives in subsequent bail jurisprudence. The Court also held that the Enforcement Case Information Report (ECIR), the ED's internal record of the commencement of investigation, is not the equivalent of a First Information Report under the Code of Criminal Procedure and need not be furnished to the accused as of right.

For hawala-related prosecutions, Vijay Madanlal Choudhary is significant on two counts. First, by affirming that money laundering is a standalone offence, it allows ED action against hawala-linked laundering to proceed even where the predicate offence prosecution is delayed or contested, which is common where predicate offences involve foreign public officials or offshore actors beyond the reach of Indian criminal process. Second, by upholding the reverse burden and the non-disclosure of the ECIR, it preserves the ED's investigative flexibility in cases built on financial-forensic and

[5] LiveLaw, '6.42% Conviction Rate In Cases Filed By ED Since 2019: Union Government Tells Parliament' (LiveLaw, 11 December 2024) <https://www.livelaw.in/top-stories/enforcement-directorate-conviction-rate-ed-pmla-278014> accessed 27 August 2026.

intelligence-led evidence, of the kind increasingly generated by blockchain analytics and transaction-pattern analysis in digital hawala investigations.

B. The Post-2022 Trajectory: Recalibrating Due Process

Subsequent decisions have qualified aspects of Vijay Madanlal Choudhary without disturbing its core holdings. *In Pankaj Bansal v. Union of India (2023),* the Supreme Court held that grounds of arrest under Section 19 must be furnished to the accused in writing, refining the informational asymmetry that Vijay Madanlal Choudhary had left largely to executive discretion. *In Prem Prakash v. Union of India (2024*) and related decisions, the Court has emphasised that 'bail is the rule and jail the exception' even within the twin-conditions framework, cautioning against prolonged pre-trial incarceration where trials are unlikely to conclude expeditiously. Review petitions challenging the correctness of Vijay Madanlal Choudhary principally on the non-supply of the ECIR and the reverse burden under Section 24 remain pending before the Supreme Court, and the Court has indicated that only these two issues, rather than a wholesale re-examination of the judgment, will be considered.

This trajectory is instructive for the present inquiry: Indian courts have been willing to sustain the PMLA's strong investigative and asset-freezing tools against the backdrop of serious, often transnational financial crime, while incrementally tightening procedural safeguards around arrest and pre-trial detention. Any technology-driven reform of the PMLA's approach to digital hawala for instance, expanded data-sharing or algorithmic transaction-monitoring mandates will need to be designed with this jurisprudential trajectory in mind, since measures that further dilute transparency to the accused are likely to invite the same due-process scrutiny that has already reshaped Sections 19 and 45 in practice.

VI. FATF Recommendations and Comparative Perspectives

A. FATF Standards on Hawala and Virtual Assets

The FATF's Recommendation 14 requires jurisdictions to license or register persons providing money or value transfer services, including hawala and other informal value transfer systems, and to subject them to AML/CFT monitoring and sanction for non-compliance. Recommendation 15, substantially revised in 2019, extends the FATF's standards to virtual assets and virtual asset service providers, requiring jurisdictions to identify and assess VDA-related money laundering and terrorist financing risks, license or register VASPs, and apply the 'travel rule' requiring originator and beneficiary information to accompany virtual asset transfers above a threshold. Both recommendations are directly relevant to digital hawala, since the phenomenon sits precisely at the intersection of unregistered value transfer services and virtual assets.

B. India's 2024 Mutual Evaluation

The FATF adopted India's fourth-round Mutual Evaluation Report at its Plenary in Singapore in June 2024, publishing the report on 19 September 2024. India was placed in the *'regular follow-up*' category, a status shared by only a handful of G20 members, reflecting a high level of technical compliance across the FATF's 40 Recommendations. The report credited India's transition from a cash-based to a digital economy driven by the Jan Dhan-Aadhaar-Mobile (JAM) trinity and the growth of UPI with reducing certain money-laundering and terrorist-financing risks associated with cash and informal value transfer. At the same time, the evaluation identified hawala and cash couriers as among the most common transfer mechanisms exploited for laundering in India, and flagged the growing significance of virtual assets as an emerging risk, alongside continuing calls to expedite money-laundering prosecutions and strengthen supervision of non-financial businesses and professions such as real estate and company service providers. The Mutual Evaluation therefore validates the central premise of this paper: India's formal AML architecture is judged internationally to be robust on paper, while hawala now substantially digitised and virtual assets remain the areas of residual and growing risk.

C. Comparative Approaches

A brief comparative survey illustrates alternative regulatory postures. The United States, through the Bank Secrecy Act and FinCEN's guidance on money services businesses, treats hawaladars and informal remitters as money transmitters subject to federal registration and state licensing, with significant civil and criminal penalties for unlicensed operation; FinCEN has separately clarified that certain virtual asset intermediaries fall within the same money-transmitter framework, aligning fiat and crypto-based informal value transfer under a single supervisory lens. The United Kingdom regulates money service businesses, including hawala operators, through registration with HM Revenue and Customs and supervision under the Money Laundering

Regulations, and has extended similar registration requirements to crypto-asset businesses through the Financial Conduct Authority. The United Arab Emirates, historically a major hawala-clearing hub for South Asian remittances, introduced a formal hawala registration framework administered by its central bank alongside a dedicated virtual asset regulatory authority (VARA) in Dubai, reflecting a deliberate strategy of drawing informal and virtual value transfer into a common licensing perimeter rather than treating them as separate risk categories. Singapore's Payment Services Act similarly regulates both traditional remittance and digital payment token services under an integrated licensing regime with graduated obligations calibrated to transaction volume and risk. India's own experience with offshore virtual asset platforms lends some support to this convergence thesis: following the December 2023 compliance action against unregistered offshore exchanges, domestic platforms such as CoinDCX reported deposit increases of up to 2,000 per cent as users migrated toward FIU-registered exchanges.[6] This suggests that a credible registration and enforcement perimeter, even one built through indirect mechanisms such as platform-blocking rather than a dedicated licensing statute, can meaningfully redirect activity toward supervised channels.

The common thread across these comparators is regulatory convergence: rather than maintaining separate, parallel regimes for informal remittance and virtual assets, more advanced frameworks increasingly apply a unified licensing, KYC, and travel-rule architecture across both channels, on the basis that digital hawala operators will otherwise arbitrage the gap between the two regimes. India's approach extending PMLA reporting obligations to VDASPs by executive notification in 2023, while continuing to police unregistered hawala principally through the residual reach of FEMA and the Fugitive Economic Offenders Act rather than a dedicated money-transmitter licensing statute is comparatively fragmented, and is discussed further in Part VII below.

VII. Regulatory Gaps in Addressing Digital Hawala

[6] Business Standard, 'Crypto Players See Surge in Activity After Crackdown on Global Companies' (Business Standard, 14 January 2024) <https://www.business-standard.com/amp/markets/cryptocurrency/indian-crypto-players-see-surge-in-users-as-meity-blocks-offshore-entities-124011400392_1.html> accessed 27 August 2026.

Read together, the statutory, institutional, judicial, and comparative material examined above discloses five principal gaps in the PMLA's capacity to address digital hawala.

1. Absence of a dedicated money-value-transfer licensing regime. Unlike the FATF's Recommendation 14 model adopted in the US, UK, and UAE, India has no standalone registration requirement specifically targeting money or value transfer service providers, including informal hawala operators. Hawala continues to be addressed indirectly, through FEMA's prohibition on unauthorised remittance and the PMLA's predicate-offence-linked laundering provisions, rather than through a dedicated licensing and supervisory perimeter analogous to that applied to VDASPs since 2023.

2. Peer-to-peer and offshore VDA activity outside the reporting-entity net. The March 2023 notification captures VDASPs as reporting entities but cannot, by its nature, reach non-custodial peer-to-peer transfers or offshore exchanges accessible to Indian users without an Indian establishment, leaving a significant channel for digital hawala settlement outside FIU-IND's visibility.

3. Fragmented, largely manual inter-agency data correlation. STR analysis by FIU-IND, blockchain forensics by the ED, telecom and platform data held by law enforcement, and tax data held by the CBDT are not systematically fused in near-real time, limiting the ability to detect the low-value, high-frequency, multi-account transaction patterns characteristic of digital hawala before value is dissipated. The scale of the underlying detection challenge is considerable: between September 2024 and January 2026 alone, the Indian Cyber Crime Coordination Centre shared details of more than 2.73 million suspected Layer 1 mule accounts with financial institutions, helping block transactions worth over Rs 9,518 crore.[7] Yet a 2024 Parliamentary Standing Committee report found that of the Rs 2,294.79 crore lost to cyber fraud in 2022, only Rs 0.57 crore was ultimately returned to victims, illustrating that detection volume does not by itself translate into timely asset recovery absent faster cross-agency correlation.

[7] The420.in, 'India's Digital Fraud Network Expands: Over 524,000 Mule Accounts Flagged in March 2026' (The420.in, 10 July 2026) <https://the420.in/india-mule-accounts-upi-fraud-march-2026-report/> accessed 27 August 2026.

4. Cross-border evidentiary and asset-recovery delays. MLAT and international cooperation timelines remain slow relative to the speed of digital value transfer, and freezing or repatriating VDA-denominated proceeds held on offshore exchanges or in self-custodied wallets remains procedurally and technically difficult even where the ED can identify the relevant wallet cluster.

5. Due-process tension in any expansion of surveillance-style tools. Given the Supreme Court's post-2022 emphasis on written grounds of arrest and bail as the norm, any reform introducing broader algorithmic monitoring, data-sharing, or lowered evidentiary thresholds for digital hawala detection must be calibrated against this jurisprudential direction, or risk both constitutional challenge and erosion of the PMLA's institutional legitimacy.

VIII. Towards Reform: Technology-Driven and Institutional Measures

Addressing these gaps requires reform along three complementary tracks: technological, institutional, and international.

A. AI-Enabled Financial Intelligence

FIU-IND and reporting entities should be encouraged, through regulatory guidance issued under the PML Rules, to deploy machine-learning-based transaction-monitoring systems capable of detecting structuring, mule-account clustering, and cross-channel patterns (bank-to-wallet-to-VDA chains, for instance) that individually fall below suspicion thresholds but collectively indicate hawala-style netting. Blockchain analytics capability within the ED and FIU-IND should be institutionalised and resourced on a standing basis, rather than procured on a case-by-case basis, given the centrality of wallet-clustering analysis to VDA-based hawala investigations. Some of this technological capacity is already emerging outside the PMLA framework: the Reserve Bank of India has been developing a Digital Payments Intelligence Platform, and banks have separately deployed the MuleHunter.AI tool, both designed to flag suspicious accounts using pooled bank, telecom, and cybercrime-portal data.[8] Rather than building comparable capability afresh, FIU-IND

[8] The420.in, 'RBI's New Weapon: "DPIP" the AI Platform That Will Spot Digital Fraud Before They Can Happen' (The420.in, 14 October 2025) <https://the420.in/rbi-ai-digital-payment-fraud-detection-dpip/> accessed 27 August 2026.

and the ED could plausibly interoperate with these RBI-led initiatives, reducing duplication between the fraud-prevention architecture developing around digital payments and the laundering-detection mandate that the PMLA already assigns to FIU-IND and the ED.

B. Strengthening Compliance and Closing the Licensing Gap

A dedicated statutory or regulatory framework for money and value transfer services, modelled on FATF Recommendation 14 and comparable to the frameworks in the US, UK, and UAE, would bring informal remitters within a defined registration and supervisory perimeter, making unregistered hawala activity independently sanctionable rather than reachable only through FEMA or a PMLA predicate offence. Complementarily, the VDA reporting-entity regime should be extended, so far as jurisdictionally feasible, to capture VDASPs marketing services to Indian residents from offshore, consistent with the extraterritorial reach already recognised in FEMA.

C. Inter-Agency Coordination and a Unified Financial Intelligence Layer

A structured, technology-enabled data-fusion mechanism linking FIU-IND, the ED, RBI, SEBI, CBDT, and state economic offences wings — with appropriate statutory safeguards on access, purpose limitation, and audit — would materially improve the detection of dispersed digital hawala patterns. Existing MoU-based cooperation should be placed on a firmer statutory footing with defined data-sharing timelines, and periodic joint typology exercises (of the kind FATF itself conducts) should be institutionalised to keep detection methodologies current with evolving hawala-digitisation techniques.

D. Enhanced Cross-Border Cooperation

India should continue to deepen its engagement with the Egmont Group for expedited FIU-to-FIU intelligence exchange, and pursue bilateral and regional arrangements particularly with UAE, Gulf, and Southeast Asian jurisdictions that are significant nodes in South Asian hawala and remittance corridors for accelerated asset freezing and information exchange in digital hawala cases, supplementing the slower MLAT process with FIU-level and regulator-level cooperation channels where available.

E. Preserving Due Process

Any expansion of monitoring or data-sharing powers should be accompanied by clear statutory purpose limitation, judicial or independent oversight of algorithmic flagging systems, and continued adherence to the disclosure standards the Supreme Court has read into Sections 19 and 45 since 2022. Reform that strengthens detection without correspondingly strengthening procedural safeguards risks both constitutional vulnerability and erosion of public confidence in the PMLA's legitimacy an outcome that would be self-defeating given that FATF's own evaluation methodology increasingly weighs effectiveness against fundamental rights protections.

IX. Conclusion

The PMLA, 2002, as interpreted and enforced through the ED and FIU-IND and tested by the Supreme Court in Vijay Madanlal Choudhary and its progeny, provides India with a formally robust anti-money laundering architecture, a conclusion borne out by India's 'regular follow-up' status in the FATF's 2024 Mutual Evaluation. Yet the same evaluation, and the analysis undertaken in this paper, confirms that hawala now substantially reconstituted through fintech rails, virtual digital assets, trade-based settlement, and encrypted coordination remains India's most persistent laundering vulnerability. The statutory extension of reporting obligations to virtual digital asset service providers in 2023 was a necessary and internationally consistent step, but it addresses only the intermediated segment of digital hawala, leaving peer-to-peer, offshore, and hybrid fiat-crypto settlement largely outside the reporting net.

Closing this gap will require India to move from a predicate-offence-anchored, intermediary-by-intermediary compliance model towards a more integrated architecture: a dedicated licensing regime for money and value transfer services, AI-enabled and blockchain-forensic financial intelligence capability embedded within FIU-IND and the ED, statutorily structured inter-agency data fusion, and deeper cross-border cooperation calibrated to the speed of digital value transfer. None of this can be pursued at the expense of the due-process safeguards that Indian courts have progressively strengthened since 2022; indeed, the durability of any reform will depend on its ability to reconcile enforcement effectiveness with constitutional fairness. Modernising the PMLA along these lines is not merely a matter of statutory housekeeping but a precondition for India to keep pace with a laundering methodology that has already moved decisively into the digital domain.

References

1. Prevention of Money Laundering Act, 2002 (India).
2. Foreign Exchange Management Act, 1999 (India).
3. Fugitive Economic Offenders Act, 2018 (India).
4. Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (India).
5. Ministry of Finance, Department of Revenue, Notification No. S.O. 1072(E), 7 March 2023 (bringing virtual digital asset activities within the PMLA reporting-entity framework).
6. Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929.
7. Pankaj Bansal v. Union of India, (2024) 2 SCC 1.
8. Prem Prakash v. Union of India through the Directorate of Enforcement, 2024 SCC OnLine SC 2270.
9. Nikesh Tarachand Shah v. Union of India, (2018) 11 SCC 1.
10. Financial Action Task Force, Mutual Evaluation Report: Anti-Money Laundering and Counter-Terrorist Financing Measures - India (FATF, Paris, adopted June 2024, published 19 September 2024).
11. Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations (FATF, Paris, as updated).
12. Enforcement Directorate, Government of India, International Cooperation and FATF, available at the Enforcement Directorate's official website.
13. Financial Intelligence Unit-India, Ministry of Finance, Government of India, official reporting and compliance guidance.
14. Press Information Bureau, Government of India, 'FATF Adopts Mutual Evaluation Report of India in its June 2024 Plenary Held in Singapore' (28 June 2024).
15. Bank Secrecy Act, 31 U.S.C. § 5311 et seq. (United States); FinCEN guidance on money services businesses and convertible virtual currencies.
16. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (United Kingdom).
17. Payment Services Act 2019 (Singapore).
18. Central Bank of the United Arab Emirates, Hawala Providers Regulation; Virtual Assets Regulatory Authority (VARA), Dubai.