REGULATORY ENFORCEMENT IN INDIA'S VIRTUAL ASSET SECTOR

I. INTRODUCTION: THE DEATH OF THE "REGULATORY VACUUM"

March 7, 2023, is a watershed moment in the landscape of Indian financial regulation. A groundbreaking notification by the Ministry of Finance had brought Virtual Digital Asset activities within the fold of the Prevention of Money Laundering Act, 2002. [1]This strategic step marked the end of the era of "regulatory ambiguity" for the crypto sector in India. By bringing into place a stringent, activity-based Anti-Money Laundering and Counter-Financing of Terrorism regime, the Indian government has given a clear signal that crypto might not be banned, but it must operate in a transparent, accountable, and thoroughly monitored legal ecosystem.

A. Watershed Moment: Notification S.O. 1072(E)

The 2023 Notification was more than a procedural update; it was a jurisdictional land-grab by the Department of Revenue. By applying powers under Section 2(1)(sa)(vi) of the PMLA, the Central Government defined any person undertaking an activity related to VDA (that is, exchange, transfer, safekeeping, administration, or custody) as a “Reporting Entity.” [2] This instantly switched the onus of policing the often-opaque and vast world of digital assets from the state onto the service providers themselves.

B. From Prohibition to Oversight: The Judicial Bridge

This "regulation through enforcement" approach represents a mature shift from RBI's earlier stance. Back in 2018, RBI tried to impose an outright "banking ban" on crypto, which was duly struck down by the Supreme Court in Internet and Mobile Association of India v. Reserve Bank of India.[3] The Court held that the blanket ban was disproportionate to the evidence of no apparent direct harm to regulated banks. However, it did not deny the power of the State to regulate.

Moreover, while the prohibition of RBI was held to be an "unreasonable restriction" under Article 19(1)(g) of the Constitution,[4] the incorporation of VDAs within the PMLA regime has been emboldened by the Supreme Court’s judgment in Vijay Madanlal Choudhary v. Union of

---

[1] Ministry of Finance (Dep’t of Revenue), Notification S.O. 1072(E) (Mar. 7, 2023).
[2] Id.
[3] Internet and Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 SCC 274 (India).
[4] lNDIA CONST. art. 19, cl. 1(g).

India, in 2022, where the stringent powers under the PMLA had been upheld as a needed tool against “the menace of money laundering.” [5]

Thesis Statement Inclusion of VDAs under the PMLA is not a mere compliance update but a conceptual leap that gives crypto exchanges the same systemic weight as traditional banking institutions. This article argues that the present regime constitutes a "sovereign reclaiming" of the digital financial space, in which participation in markets is strictly conditional on total transparency and unconditional cooperation with the state's investigative machinery.

II. DECONSTRUCTING THE VASP DEFINITION UNDER PMLA

The regulatory architecture introduced by the 2023 Notification departs from labeling certain entities, such as "exchanges" or "wallet providers," and instead takes on an approach of being functional and activity-based. This makes sure that any technological evolution of the sector does not fall outside the regulatory net just because of changes in nomenclature.

A. The "Activity-Based" Paradigm under Section 2(1)(sa)(vi)

The legal basis for this oversight is provided under Section 2(1)(sa)(vi) of the PMLA, which thus empowers the Central Government to mandate any person undertaking “designated business or profession” as a Reporting Entity (RE).[6] Classifying VDA-related activities under this section, the government harmonized India’s domestic law with the FATF Standards, Recommendation 15 dealing with “New Technologies.”[7]

B. The Five Pillars of VASP Activity

The Notification names five activities below which, if performed on behalf of another person "in the course of business," render RE status:

1. Exchanging between VDAs and fiat currencies: The main "on-ramp" and "off-ramp" services.
2. Trading between one or more types of VDAs, also generally referred to as "crypto-to-crypto" trading.
3. VDA transfers: Transferring digital assets between two different addresses or accounts.
4. Custodianship or administration of VDAs: This encompasses custodial wallet providers and those maintaining "instruments enabling control" over VDAs.

---

[5] Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929 (India).

[6] Prevention of Money Laundering Act, 2002, § 2(1)(sa)(vi), No. 15, Acts of Parliament, 2003 (India).

[7] FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 24 (2021).

5. Providing financial services connected to an issuer's offer and sale of a VDA: The focus is on the target Initial Coin Offering (ICO) and token sales.[8]

C. The "Instruments Enabling Control" & the DeFi Challenge

Perhaps the most legally contentious phrase in the notice is “instruments enabling control over VDAs.” The broad use of language here aims to catch, not only those who have private keys, but also smart contract or multi-signature protocol administrators that could change or freeze the functionality of a digital asset. This leaves significant grey area for DeFi. To the extent a protocol is truly immutable and non-custodial, one could argue there is no “person” to hold liable, but any project retaining “admin keys” or “governance levers” is probably a form of “administration.”[9] Thus, it would appear developers retaining significant control over a protocol's economic parameters may qualify as VASPs, regardless of the "decentralized" label.

III. THE COMPLIANCE "TRIAD": KYC, MAINTENANCE, AND REPORTING

VASPs being treated as Reporting Entities would, therefore, attract the full force of the statutory compliance regime under Chapter IV of the PMLA. This is a regime of creating a "digital paper trail" that may be audited at will by the FIU-IND and the ED. This burden essentially rests on three pillars: Customer Due Diligence, Record Maintenance, and Mandatory Reporting.

A. Customer Due Diligence-KYC and the Risk-Based Approach

Under Section 12AA of the PMLA, VASPs are obligated to identify clients by applying a risk-based approach before undertaking a business relationship.[10] This should include:

- *Verification:* Obtaining Aadhaar, PAN, or any other Officially Valid Documents and verifying the same with the Central KYC Registry.

- *Enhanced due diligence:* EDD applies to higher-risk transactions, such as those involving PEPs or customers from the FATF “Grey List” countries, in which case VASPs should further investigate a customer's “ownership and financial position, including sources of funds”.[11]

- *Beneficial Ownership:* VASPs are legally obliged to look through corporate veils to identify the natural persons who ultimately own or control the digital assets.

[8] Ministry of Finance (Dep’t of Revenue), Notification S.O. 1072(E) (Mar. 7, 2023).
[9] GLOBAL LEGAL INSIGHTS, BLOCKCHAIN & CRYPTOCURRENCY LAWS AND REGULATIONS 2026: INDIA (2025).
[10] Prevention of Money Laundering Act, 2002, § 12AA, No. 15, Acts of Parliament, 2003 (India).
[11] Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Rule 9 (India).

B. The Record-Keeping Burden: Section 12 Obligations

Some of the biggest operational challenges facing VASPs are the requirements to retain records of all transactions.

Record Keeping: S. 12(3) mandates records to be kept for at least five years from the date of transaction or five years after the end of the business relationship.[12]

Reconstructive capability: These records shall be sufficient to "permit reconstruction of individual transactions, including the amounts and types of currency involved."[13] For blockchain-based businesses this implies that VASPs must map off-chain KYC data onto on-chain wallet addresses, a technically demanding and resource-intensive task.

C. Transaction Monitoring and Reporting Dynamics

The last pillar is the active reporting of data to the FIU-IND. VASPs have to designate a Principal Officer and a Designated Director who will be in charge of this reporting.

Suspicious Transaction Reports: VASPs are required to file an STR within seven working days of forming a "reasonable ground of suspicion" that a transaction involves proceeds of crime, regardless of the value of the transaction.[14]

Threshold-based reporting: Even though STRs are value-neutral, VASPs are also required to file CBWTRs for all cross-border wire transfers of more than ₹ 5 lakh, or its equivalent in foreign currency, in cases where either the origin or destination is in India.[15]

Failure to uphold these pillars attracts not only administrative fines but also, upon the interpretation of the Supreme Court in Vijay Madanlal Choudhary, constitutes an act of facilitating money laundering with its rigorous bail conditions under the PMLA and a possible attachment of corporate assets against the VASP's directors.[16]

---

[12] Prevention of Money Laundering Act, 2002, § 12(3)-(4), No. 15, Acts of Parliament, 2003 (India).
[13] Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Rule 3 (India).
[14] *Id.* Rule 7.
[15] FIN. INTELLIGENCE UNIT-INDIA, AML & CFT GUIDELINES FOR REPORTING ENTITIES IN VDA SECTOR 18 (2023).
[16] Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929 (India).

IV. EXTRATERRITORIALITY AND THE CRACKDOWN ON OFFSHORE ENTITIES

The most commercially consequential feature of India's VDA regulatory framework is its unapologetic extraterritorial application. The FIU-IND has variously reiterated that the obligation to register as a Reporting Entity is "activity-based" and is not dependent upon either a physical presence or a registered office within the territory of India.[17] This position stipulates that any offshore exchange catering to the Indian market must indeed comply with the PMLA-a clear extension of India's sovereign regulatory reach into the global digital commons.

A. Principle of Domicile Neutrality

The definition of "Reporting Entity" under the PMLA does not carve out a domestic incorporation requirement.In case there is a facilitation of VDA transactions by a platform for and to Indian residents, it will be said to be "carrying on a designated business" in India. This would, however, follow the increasing trend in "long-arm" financial regulation around the world, where the applicability of law is a function of the locus of the consumer, not of the server. For offshore VASPs, this would create a binary choice: formalize operations through registration or face systemic exclusion from the Indian market.

B. Case Study: The 2024-2025 Enforcement Wave

In December 2023, the FIU-IND initiated a decisive enforcement action by issuing show-cause notices to nine major offshore exchanges, including Binance, KuCoin, and Huobi, for failing to comply with PMLA registration requirements.[18]

The repercussions of non-compliance were swift and serious. At the recommendation of the FIU, MeitY employed its powers under Section 79(3)(b) of the Information Technology Act, 2000 to ban the URLs and mobile applications of these exchanges.[19] This "digital embargo" effectively severed access to the Indian user base, thus making compliance a commercial necessity rather than a legal preference.

---

[17] FIN. INTELLIGENCE UNIT-INDIA, COMPLIANCE COMMUNIQUE FOR VDA SERVICE PROVIDERS 4 (2023).
[18] *Press Release: FIU IND Issues Show Cause Notices to Nine Offshore Virtual Digital Asset Service Providers*, MINISTRY OF FIN. (Dec. 28, 2023), https://pib.gov.in/PressReleasePage.aspx?PRID=1991334.
[19] Information Technology Act, 2000, § 79(3)(b), No. 21, Acts of Parliament, 2000 (India).

In June 2024, Binance, the world's largest exchange, was slapped with a landmark penalty of ₹18.82 crore ($2.25 million) for operating in violation of PMLA obligations.[20] Similarly, in early 2025, Bybit received a penalty of ₹9.27 crore after its attempt to re-enter the market.[21] In fact, these penalties are "entry fees" for these offshore giants looking to legitimize their presence in India's high-volume market, rather than simply punitive measures.

Legal Liability and Criminal Risk Apart from corporate fines, the PMLA casts personal liability. Section 70 of the Act provides that if a company contravenes the law, every person who at the time of contravention was in charge of and was responsible to the company for the conduct of its business shall be deemed guilty.[22] This has implications for offshore directors in terms of lookout circulars and possible arrest upon entry into India, which further specifies the gravity of the mandate of FIU.

V. THE "GRAY ZONES": DEFI, SELF-CUSTODY, AND THE REVERSE BURDEN OF PROOF

First, there are certain "gray zones" where technology has gotten ahead of the current legal text as India is moving from a situation of regulatory vacuum to high compliance. These are areas of greatest risks for investors and most complex advisory challenges for legal counsels.

A. DeFi and Self-Custody: A Paradox

The PMLA Notification frames obligations around activities carried out "for or on behalf of another person."[23] This creates an immediate enforcement hurdle for Decentralized Finance (DeFi) and non-custodial wallets-e.g., MetaMask, hardware wallets like Ledger.

- The Intermediary Problem: In a truly decentralized exchange, there is no "person" or central intermediary to be registered as a Reporting Entity. Users interact with smart contracts.

- Self-Custody: persons in possession of their own private keys do not fall under the definition of a VASP because they are not offering a service to "another person." However, the lack of an intermediary means that should these assets be deemed "proceeds of crime," the individual has no institutional buffer to provide a compliance trail.

---

[20] *In re* Binance, Order in Original No. 10/DIR/FIU-IND/2024 (Financial Intelligence Unit-India, June 19, 2024).
[21] *In re* Bybit, Order in Original No. 02/DIR/FIU-IND/2025 (Financial Intelligence Unit-India, Jan. 14, 2025).
[22] Prevention of Money Laundering Act, 2002, § 70, No. 15, Acts of Parliament, 2003 (India).
[23] Ministry of Finance (Dep't of Revenue), Notification S.O. 1072(E) (Mar. 7, 2023).; GLOBAL LEGAL INSIGHTS, BLOCKCHAIN & CRYPTOCURRENCY LAWS AND REGULATIONS 2026: INDIA (2025).

- Regulatory Stance - 2025: The FIU-IND has clarified that while "immutable code" cannot be a reporting entity, developers or governance DAO members maintaining "admin keys" or "control levers" may be classified as VASPs if they actively facilitate transactions.

B. Section 24: The Reverse Burden of Proof

Perhaps the most daunting aspect of the PMLA for VDA holders is Section 24, which creates a legal presumption that is rare in traditional criminal law.

- Presumption: In any proceedings relating to "proceeds of crime," the Authority or Court shall presume that such proceeds are involved in money laundering until the contrary is proved. [24]

- Impact on Crypto: Due to the fact that blockchain transactions are pseudonymous in nature, an individual may receive "tainted" crypto from some third party without knowing its origin. Under Section 24, the burden is not on the ED to prove the user's guilt but on the user to prove that the assets are untainted property.[25]

- Judicial Validation: In this regard, the Supreme Court in Vijay Madanlal Choudhary upheld the reverse burden, thus stating that since the facts regarding the source of funds are within the "special knowledge" of the accused, it is constitutional to require them to explain the source.[26]

C. "The Tainted Asset" Contagion

Law firms increasingly advise clients about the risk of "tainted" assets. If a VASP's wallet is "dusted" with tokens originating from a hack or a prohibited jurisdiction, the entire wallet can be flagged. Without a potent TMS utilizing blockchain forensics (e.g., Chainalysis or Elliptic), a VASP may innocently breach its PMLA obligations by simply facilitating a P2P transfer.[27]

VI. COMMERCIAL IMPLICATIONS AND THE EVOLVING ROLE OF LEGAL COUNSEL

[24] Prevention of Money Laundering Act, 2002, § 24, No. 15, Acts of Parliament, 2003 (India).
[25] Kings & Alliance LLP, *The Intersection of PMLA and Digital Assets*, KNALLP (2024), .
[26] Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929 (India).
[27] FIN. INTELLIGENCE UNIT-INDIA, AML & CFT GUIDELINES FOR REPORTING ENTITIES IN VDA SECTOR 21 (2023).

Moving from an unregulated "wild west" to a high-compliance regime has fundamentally changed the commercial calculus for the Indian VDA sector. Far from stifling the industry, the PMLA framework has brought in a degree of institutional legitimacy that was hitherto absent, thereby creating operational burdens but also strategic opportunities.

A. Compliance as a Barrier to Entry and Consolidation

The cost of compliance under PMLA-including the implementation of robust KYC/AML software, periodic cyber security audits by CERT-In empanelled auditors, and the appointment of dedicated compliance officers-is fairly significant. This "regulatory tax" has proved prohibitive for smaller startups and has ensured a visible consolidation of the market. Only well-capitalized entities able to sustain this overhead are surviving, thereby effectively increasing the barrier to entry.

B. The "Compliance Dividend" and Banking Access

The "un-banking" of crypto firms began to reverse following the 2020 IAMAI judgment and the 2023 PMLA notification. Regulated exchanges demonstrating FIU-IND registration and strict adherence to the FATF Travel Rule are finding it increasingly easy to secure traditional banking partnerships.[28] This "compliance dividend" is critical for business continuity, as it allows for smoother fiat-to-crypto on-ramping—the lifeblood of any retail-facing exchange.

C. Strategic Advisory: A New Practice Area for Law Firms

This PMLA enforcement wave has spawned a very lucrative advisory niche for top-tier law firms. No longer does one just litigate against bans; law firms have now become critical partners in the following:

- Regulatory Onboarding: Helping domestic and offshore VASPs through a new registration process with the FIU-IND, which now has more stringent "fit-and-proper" criteria as well as mandatory cybersecurity certifications.[29]

- White-Collar Defense: Representing entities under investigation by the Directorate of Enforcement and responding to show-cause notices for facilitating "tainted" transaction flows.

[28]AZB & Partners, *Virtual Currency Regulation Review 2025*, AZB & PARTNERS (June 12, 2025), .
[29] Fin. Intelligence Unit-India, F.No. 9-8/2023/COMPL/FIU-IND-Pt-II (Sept. 15, 2025).

- Product Structuring: Advising FinTech firms on whether new products (e.g., tokenized RWAs and liquidity staking protocols) trigger VASP status under the "instruments enabling control" test.[30]

VII: CONCLUSION - TOWARD A PERMANENT LEGISLATIVE FRAMEWORK

The evolution, therefore, of India's virtual asset regulation from 2023 to 2025 represents a philosophy of "regulation through enforcement." By adopting the PMLA as the major tool for oversight, the Indian state has effectively brought under sovereign control a decentralized technology without an outright ban.

The current reliance on anti-money laundering statutes is, if anything, a "bridge" rather than a destination. To date, the PMLA has served to reduce financial crime, but none of the preceding laws address consumer protection, market conduct, and the systemic risks associated with stablecoins. The consistent urgings of the Supreme Court for a comprehensive bill indicate that a more holistic Crypto Regulation Bill (COINS Act) still awaits. [31]

Eventually, the formalization of the VDA sector is an irreversible trend. By 2025, merely technical innovation is no longer sufficient to provide a legitimate operation baseline in India; it has to be an ability to operate transparently within the bounds of the law. The message is clear: in the new Indian crypto landscape, compliance is the most valuable asset for both the practitioner and participant.

---

[30] Global Legal Insights, *Blockchain & Cryptocurrency Laws and Regulations 2026: India*, GLOBAL LEGAL INSIGHTS (Oct. 21, 2025), .

[31] FinLaw India, *Cryptocurrency Law in India: Current Legal Status and Regulatory Landscape (2025)*, FINLAW.IN (Nov. 2025), .