FIU-IND Annual Report FY 2024-25 | New AML/KYC norms for crypto exchanges in India and other news

February, 2026

FIU-IND Annual Report FY 2024-25

By Shivani S.

Financial Intelligence Unit - India recently published its Annual Report for FY 2024-25, which covers recent trends in regulatory reporting, compliance framework and enforcement actions in India. In addition to the changes in the volume of reports, the report highlights the growing importance of virtual asset service providers and has subsequently introduced new KYC norms related to them.

© Navigate Consulting Pvt.Ltd.

Key takeaways include

- The total number of Cash Transaction Reports (CTRs) witnessed a marginal decline, decreasing from 1,81,27,460 in FY 2023-24 to 1,73,13,368 in FY 2024-25.
- Suspicious Transaction Reports (STRs) saw a significant increase, rising from 3,68,592 in FY 2023-24 to 4,34,668 in FY 2024-25, although the number remains lower than 6,45,905 reports filed in FY 2022-23.
- Cross Border Wire Transfer Reports (CBWTRs) increased substantially from 90,87,189 to 1,02,73,512.

These upward trends in STRs and CBWTRs reflect improved detection capabilities and heightened vigilance by reporting entities in identifying potentially suspicious and cross-border financial activities.

FIU-India also played a critical role in improving enforcement outcomes by disseminating 6,908 priority STRs to various law enforcement agencies (LEAs) during FY 2024-25, a sharp rise from 2,750 priority STRs disseminated in FY 2023-24. This increase is primarily due to the increase in reporting entities covered under the priority intimation framework, as well as the enhanced quality of reports, over 40 per cent of which were found to be useful by LEAs for investigative and enforcement purposes.

An aggregate penalty of ₹30,48,65,000 was levied during the year for regulatory non-compliance. These enforcement actions emphasised the lack of timely detection, escalation, and reporting of anomalous transactions. According to the report, financial institutions should have systems in place to avoid such enforcement actions. This includes rigorous verification of customer identity and authority through robust Know Your Customer (KYC) processes, comprehensive due diligence procedures, effective alert

generation and transaction screening mechanisms, strong oversight and data governance frameworks.

Reporting entities are also expected to develop and implement comprehensive AML/CFT policies, supported by internal systems for STR filings, customer risk classification, and ongoing monitoring, ensuring compliance with regulatory expectations and protection from financial crime risks.

Source: FIU-IND

REGULATORY UPDATE

FIU-IND strengthens AML/KYC norms for crypto exchanges

By Adhila Thirumalai

On 8th January 2026, India's recent Financial Intelligence Unit (FIU) report introduced certain stringent AML & KYC norms for cryptocurrency exchanges, addressing the rise of financial fraud through these exchanges. As per the updated framework, crypto exchanges have been classified as Virtual Digital Asset (VDA) service providers. The FIU is the single-point regulator for cryptocurrency exchanges operating in India under the Prevention of Money Laundering Act, 2002.

The FIU-IND strengthens the KYC and risk management framework through the following norms

© Navigate Consulting Pvt.Ltd.

- Live selfie using software that verifies physical presence through features such as eye-blinking or head movement, a step aimed at preventing the use of static images or deepfakes.
- Mandatory geographical tracking during user onboarding.
- Submission of secondary identity documents such as a passport, Aadhar, or Voter ID, and OTP verification of email id and phone number.
- Capture of geo-location (latitude & longitude), IP address, date, and timestamp at the time of account creation
- Mandatory penny-drop (Rupee 1) verification to validate bank account ownership and operability of the registrant.
- Mandatory KYC updation for high-risk customers every six months and annually for other customers.
- EDD for high-risk customers, including PEPs, NPOs on the FATF black or grey list.
- VDA service providers must abide by all requirements outlined in the PMLA and its implementing regulations that apply to reporting entities.

Due to increased money laundering(ML), terrorist financing(TF) and fraud threats, the FIU-IND mandated sanction screening to be done each time a VDA transaction is initiated and has also taken a strong stand against systems that hide the trail of cryptocurrency transactions, prohibiting involvement in or facilitation of Initial Coin Offerings (ICOs) and Initial Token Offerings (ITOs). FIU has also instructed exchanges to maintain client information, including address and transaction details, for at least five years and until the end of any investigation. These guidelines by the FIU-IND help in fostering a secure, regulated environment for Virtual Digital Assets.

Source: FIU-IND

© Navigate Consulting Pvt.Ltd.

NEWS SNIPS FROM AROUND THE WORLD

[Collated from other publishers and sources from the Internet, as referenced after each snippet]

Nine sentenced in major gambling and money laundering case

Kuwait's Criminal Court has sentenced nine individuals to seven years in prison each and imposed fines of KD1 million per person after finding them guilty of forming an organised criminal network that operated an online gambling platform and laundered illegal proceeds. A company involved was fined over KD1.839 million and banned from all commercial activity. Investigations revealed that gambling revenues were funnelled through bank accounts belonging to a medical clinic and several commercial entities, where they were falsely recorded as legitimate income before being recycled and transferred abroad to obscure their illegal source.

© Navigate Consulting Pvt.Ltd.

Source: Gulf News

Bank of Scotland fined for sanctions breach involving former Russian official

Bank of Scotland, part of Lloyds Banking Group, was fined £160,000 by the UK's Office of Financial Sanctions Implementation (OFSI) for breaching sanctions after opening and operating a bank account for a sanctioned individual. The account belonged to Dmitrii Ovsyannikov, a former senior Russian government official who has been on the UK sanctions list since 2017. In February 2023, the bank processed 24 transactions worth about £77,000 through the account. Ovsyannikov used a British passport with a spelling variation of his name, which led to the sanctions screening failure. Since Lloyds voluntarily reported the issue in March 2023, the fine was reduced by half. Ovsyannikov, who became a British citizen in January 2023, was sentenced to 40 months in prison last year for breaching UK sanctions and money laundering.

Source: Reuters

CBI uncovers ₹1,600 crore cybercrime scam using mule accounts

The CBI discovered a massive financial scam in which the proceeds of cybercrime and other illegal acts were concealed, layered, and transferred through the systematic creation of mule bank accounts, with transactions totalling more than ₹1,600 crore. By using fake KYC documents, fake identity and address proofs, and fraudulent supporting documentation, these mule accounts were formed in the names of non-existent companies, enabling account onboarding in severe violation of KYC and due diligence standards. Large amounts of money were routed, layered, and transferred between

© Navigate Consulting Pvt.Ltd.

banking and digital platforms using the accounts after they were active; the total number of transactions exceeded ₹1,600 crore.

Source: The Hindu

FCA launches Firm Checker tool to help fight financial crime

The UK's Financial Conduct Authority (FCA) has launched a new online tool called Firm Checker to help consumers verify whether a financial services firm is genuinely authorised and reduce the risk of falling victim to scams and other financial crime. Firm Checker allows members of the public to quickly search and confirm whether a company is authorised by the FCA and has the right permissions to provide the specific financial product or service being offered. By providing clear verification of a firm's regulatory status, the FCA hopes to significantly reduce the likelihood of consumers being misled by fraudulent operators posing as legitimate firms.

Source: FCA

EBA transfers AML duties to AMLA

The European Banking Authority (EBA) has officially transferred all the Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) to the Anti Money Laundering Authority (AMLA), marking a shift in the European Union's approach to combating financial crime. As part of the handover, EBA's key technical tools and expertise, including the EuReCa (EBA's AML/CFT database), supervisory insights, and risk assessments, have been transferred to AMLA. AMLA and EBA jointly aim to deliver a more effective and consistent EU response to financial crime.

Source: AMLA

Cross-border cyber fraud through mule accounts uncovered

Police uncovered a cross-border cyber fraud operation in which mule bank accounts were systematically supplied to an international scam network operating from Southeast Asia. Local people, mostly unemployed teenagers and workers, were used to open about 110 bank accounts. They were paid small amounts to hand over control of their accounts. Money from victims of cybercrime was transferred quickly across a number of accounts, converted into cryptocurrency, and sent to fraudsters overseas using these mule accounts. According to authorities, this network was used to launder approximately ₹650 crore, with middlemen receiving large commissions for helping to shift illegal money.

Source: The Times of India

Two convicted in a major £17M money laundering scheme

Two suspects were arrested in June 2021 for their role in a £17m money laundering operation in Birmingham. The operation took place across Post Office branches in the east of Birmingham, with members of the group making more than ten visits a day to deposit large amounts of cash into business bank accounts. A suspect's mobile phone contained login details for several company bank accounts where the cash deposits were being made, along with credentials for other accounts to which the money was later transferred. This allowed investigators to trace the movement of funds across multiple accounts and showed that the banking activity was being controlled from a single source. Authorities have seized a substantial amount of criminal assets as a result of the investigation, including around £867,000 via account freezing orders, plus £100,000 in cash seized at the time of arrest and another £9,000 discovered in linked searches.

Source: West Midlands Police

© Navigate Consulting Pvt.Ltd.

Navigate Consulting enables banks and financial institutions to better understand Financial Crime Management and make the most productive use of their AML and Fraud Management systems through training and knowledge sharing.

© Navigate Consulting Pvt.Ltd.

For more details write to: connect@navigate-change.com