the laundry times

Stay in the know of the latest in the world of AML and financial crime.

MONTHLY NEWSLETTER

navigate

Brought to you by Navigate Consulting,
an associate company of Quantum Data Engines

July, 2025

TOP STORY

Decentralized Wallets and Telegram: Crypto Laundering Network Uncovered

By Anna Paulin

The Uttar Pradesh Cyber Crime cell discovered a sophisticated money laundering racket involving illegal cryptocurrency trading through Telegram. The racket was run by Chinese nationals with the help of Indian proxies. In the past two months, they funneled ₹75–80 lakhs through fake ‘crypto trading’ deals without using any legitimate exchange.

The eight accused lured individuals by promising high returns on investments in crypto assets. The racket's modus operandi involved hiring Indian bank account holders (mule accounts) on a commission basis. These mule account holders were made to receive high-value deposits via “NEFT, RTGS or IMPS” which were then withdrawn in cash on the same day and handed over to underground cryptocurrency brokers. Mule account holders knowingly participated in the crime and intentionally bypassed KYC requirements.

Investigations revealed, the cryptocurrency brokers purchased USDT with the help of Decentralized peer-to-peer (P2P) wallets, which function without KYC regulations and guarantee total anonymity, making it impossible for law enforcement to track them. These decentralized wallets

operate outside the control of any single country, enabling users to hide both the origin and destination of funds.

Following purchase, USDT is transferred to the wallet addresses supplied by Telegram channels through the TRC-20 network. Telegram channels played a key role in coordinating wallet addresses, ensuring the crypto trail remained untraceable.Throughout the process, there was no evidence of invoices, valid exchange, or tax records, making it ideal for illicit money laundering.

This case is an example of how unregulated crypto tools, like decentralized wallets and messaging platforms, are enabling global financial crime. With cases like this coming into light, especially through mule accounts, there is an urgent need for cryptocurrency regulations. Without clear rules on KYC, wallet tracing, exchange accountability, and cross-border crypto flows, decentralized platforms will continue to be exploited for financial crime. Hence, a strong regulatory framework is essential to prevent financial crimes that are evolving in the digital asset space.

Source: The Times of India

NEWS SNIPS FROM AROUND THE WORLD

By Neha Joy, Anna Paulin and Shivani Shetty

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

UAE launches major money laundering crackdown

The United Arab Emirates regulators recently launched a significant crackdown on financial institutions involved in money laundering and terrorism financing, imposing penalties exceeding Dh 339 million. The action targeted a range of entities, including local exchange houses, international bank branches, and insurance companies. The primary issues identified across these institutions were deficiencies in monitoring and reporting suspicious transactions, along with shortcomings in customer verification and identifying the ultimate beneficial owners.

Source: Times of India

EU adds Monaco to high-risk jurisdiction list for money laundering

The European Commission has updated its list of high-risk jurisdictions with strategic deficiencies in anti-money laundering and counter-terrorism financing. Monaco, along with Algeria, Angola, Côte d'Ivoire, Kenya, Laos, Lebanon, Namibia, Nepal, and Venezuela, has been added to the list. Monaco is renowned for its wealthy residents and high property prices, making it a notable addition to the list due to concerns over financial transparency. These jurisdictions

are seen as having inadequate measures to combat money laundering and terrorist financing.

Source: Reuters

FinCEN sanctions three Mexican banks over cartel money laundering

The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) has accused three Mexican financial institutions, CIBanco, Intercam Banco, and Vector Casa de Bolsa for money laundering under the Fentanyl Sanctions Act and the FEND Off Fentanyl Act. This move targets their alleged roles in laundering millions for Mexican cartels and facilitating payments for fentanyl chemicals. The sanctions do not freeze assets globally, however, they prohibit U.S. transactions with their Mexican branches, isolating them from the U.S. financial system. Despite these institutions' relatively small size, the action could have large consequences due to the deep integration between Mexican and U.S. financial systems.

Source: Reuters

FATF Calls for Stronger Measures Against Terrorist Financing

The Financial Action Task Force (FATF) has strongly condemned the Pahalgam terror attack in India, highlighting that terrorism cannot flourish without money and the means to move it between supporters. The watchdog emphasized its attention will be on the effectiveness of measures that countries have put in place to combat terrorist financing. In its recent plenary, the FATF noted worrying gaps in global frameworks that allow terrorist financiers to operate unchecked. Through the mutual evaluation report, FATF aims to identify the gaps that need to be addressed. To combat terror financing, countries must implement FATF standards, enable real time monitoring and unify against the rise of global terrorism.

Source: The Indian Express

California man pleads guilty in $16M hospice fraud and money laundering scheme

A California man has pleaded guilty to laundering more than $4.6 million in illicit proceeds derived from a massive $16

million Medicare fraud scheme. According to court documents, Mihran Panosyan, worked with others to create fake hospice companies using stolen identities of foreign nationals who were no longer residing in the US. They opened fake bank accounts, created identification documents, and established a network of corporate entities that appeared legitimate on paper. These shell hospices then submitted millions of dollars in false Medicare claims for services that were never rendered and for patients who were not terminally ill.

Source: Office of Public Affairs

Crypto payment company founder charged in $500m money laundering case

Iurii Gugnin, a New York based founder of cryptocurrency companies Evita Investments and Evita Pay, has been indicted in Brooklyn on 22 federal counts tied to laundering over $500 million through U.S. banks and crypto exchanges. The indictment accuses Gugnin for wire and bank fraud, money laundering, violating the Bank Secrecy Act, operating an unlicensed money-transmitting business, and evading sanctions and export-control laws under IEEPA. His actions

reportedly included falsifying invoices and customer details and enabling transactions for sensitive U.S. technology purchases, including those tied to Russia's Rosatom, as well as luxury goods and yacht services.

Source: Office of Public Affairs

₹2,915 Crore CyberCrime reported in Karnataka

A recent study by the Centre for Cybercrime Investigation Training and Research of Karnataka CID revealed that the cryptocurrency is a major factor of money laundering linked to cybercrimes in India. In 2024 the state recorded losses of ₹2,915 crore in cybercrime cases, with ₹1,860 crore from private banks and ₹948 crore from public banks. Criminals exploited mule accounts to launder money, later converting them into crypto via P2P platforms, online casinos, and gaming apps. The lack of mandatory KYC, wallet tracing, and exchange registration has made tracing these funds difficult. The study urges India to enforce strict KYC norms, timely STR reporting, and introduce penalties for money laundering and crypto misuse.

Source: The Indian Express

REGULATORY UPDATES

RBI to combat fraud with Digital Payment Intelligence Platform (DPIP)

By Neha Joy

RBI is leading a collaborative effort to combat the growing threat of digital payment fraud through the development of

the Digital Payment Intelligence Platform (DPIP) as a Digital Public Infrastructure (DPI).
This initiative is being driven by the Reserve Bank Innovation Hub and is rapidly gaining momentum with strong participation from both private and public sector banks. The DPIP aims to enable real time data sharing, advanced fraud detection and swift preventive action across the banking ecosystem.

The idea for the platform originated from a committee chaired by former NPCI MD and CEO, A. P. Hota. Approved in mid-2024, the committee recommended a centralized data-driven system that can monitor and flag suspicious transactions by identifying common fraud patterns and behaviors across the digital payment ecosystem. This platform is highly relevant given the recently released RBI annual report that reveals how digital transaction fraud has nearly tripled ,from Rs.12,230 crore to Rs. 36,014 crore, where most of the fraud cases are from internet and card transactions in private banks and loan frauds in public banks.

A prototype of the platform is currently under development, with 5 to 10 banks collaborating in the initial phase. Once implemented, DPIP will integrate data from various sources, such as banks, payment intermediaries, and telecom

providers to detect anomalies in real time and send out alerts before transactions are completed.

Source: Economic Times

DOMAIN MATTERS

Sanctions Evasion: Challenges and Best Practices for Compliance and Risk Mitigation

By Shivani Shetty

Sanctions evasion and proliferation financing (PF) are a serious threat to global financial stability and security. As international sanctions increase, detecting and preventing PF-related activities has become complex for both governments and financial institutions. Currently, PF and sanctions evasion are commonly being detected through

SARs/STRs and sanctions screening. The following sections cover key challenges in detecting sanctions evasion and PF, along with best practices for mitigating associated risks.

Challenges for detecting PF and sanctions evasion:

- **Limited SARs/STRs reporting**

  Many countries do not use Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) for detecting PF because PF is not criminalized in those regions. Hence, reporting entities often submit reports without the necessary details to identify PF-related activities due to a lack of guidance and legal obligations.

- **Inefficient sanctions screening and false positives**

  The integration of sanctions lists into screening tools is an important step to detect suspected PF and sanctions evasion. However, some countries face difficulties with sanctions screening matches due to frequent false positives caused by issues like name variations and incomplete identification details.

- **Low PF awareness and compliance among DNFBPs**

  Designated Non-Financial Businesses and Professionals (DNFBPs) often have a poor

understanding of their PF-related obligations. This results in weak monitoring and reporting of PF activities outside the financial sector.

Best practices for mitigating risks:

- **Sanctions Screening:** Several countries require reporting entities to use automated sanctions screening systems to improve the effectiveness of SARs/STRs. These systems integrate International and/or national sanctions lists into sanctions screening systems, allowing entities to flag matches to sanctioned individuals, entities or high risk transactions using key words.

- **STRs/SARs reporting:** A positive match found during screening requires reporting entities to file SARs/STRs and inform authorities about frozen assets or transactions linked to sanctioned entities.

- **Training:** Several countries have invested in training, outreach and specialised guidance to enhance compliance and detection capabilities.

- **AML/CFT preventive measures:** To mitigate sanctions evasion, institutions can undertake measures like

customer due diligence, risk assessment, ongoing monitoring that may lead to SARs/STRs filing, training employees, negative news screening, and enhanced due diligence.

To complement these techniques, other methods can be implemented such as cross-border intelligence sharing, international cooperation, blockchain analytics and open-source intelligence.

Thus, sanctions evasion and proliferation financing can be detected through comprehensive and strong AML/CFT frameworks. Collaboration between governments and private entities could enhance detection capabilities through improved frameworks, technological investments and training.

Please write to connect@navigate-change.com to know more.