



the laundry times

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

MONTHLY NEWSLETTER



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

September, 2025

TOP STORY



Parimatch and ban on betting apps

By Anna Paulin

Parimatch, the online gaming betting app, is currently under investigation by the enforcement directorate (ED) due to its illegal operations in India. As a part of its money laundering investigation connected to Parimatch, the ED froze Rs 110 crore in mule accounts and seized 1,200 mule credit cards

across 17 locations in India. The ED stated that Parimatch lured its victims (investors) by promising high returns, thereby generating over ₹3,000 crore in a year.

The modus operandi used by Parimatch to launder money involved funnelling funds through mule accounts. To layer the money collected from users, different strategies were implemented across southern and western India.

ED discovered that in Southern India, funds transferred into mule accounts were withdrawn in cash in a specific location in Tamil Nadu. Once withdrawn, the cash was handed over to hawala operators who recharged virtual wallets linked to a UK-based firm, which were used to purchase USDT cryptocurrency via mule crypto accounts controlled by Parimatch agents.

Whereas in western India, Parimatch utilised domestic money transfer (DMT) agents to collect betting funds in mule accounts. The DMT agents made payments to the Parimatch agents via mule credit cards.

Investigations revealed some payment companies, whose Payment Aggregator applications were rejected by the RBI, still played a key role. They enabled user fund collection through their APIs, disguised as Technology Service Providers (TSPs). The TSPs supplied the APIs to Parimatch agents to onboard mule accounts registered in the names

of e-commerce or payment solution firms. These mule accounts collected funds via UPI and masked them as e-commerce refunds, chargebacks, or vendor payments, cleverly concealing their illicit origin.

The betting app deceived people with aggressive marketing and attractive prize-winning strategies, which included partnership with well-known celebrities. Since betting advertisements are banned, Parimatch promoted itself through surrogate advertisements under 'Parimatch Sports' and 'Parimatch News', using celebrity endorsements to appear legitimate.

Given the rise in financial ruin and social distress caused by gaming and betting platforms, the parliament passed "The Promotion and Regulation of Online Gaming Bill, 2025". The bill plays a crucial role in the fight against fraud and money laundering. The central government has banned multiple gaming and betting apps since 2023, and one among them is Parimatch.

The Parimatch case is a reminder of how illegal betting platforms exploit digital infrastructure, fintech loopholes, and surrogate advertising to launder massive sums of money. It also reflects the growing risks posed by unregulated online betting platforms, which move large sums of unaccounted money through complex networks.

Bringing such platforms under stricter regulatory oversight, with mandatory compliance and reporting obligations, will be crucial in strengthening financial integrity.

Source: Times of India

NEWS SNIPS FROM AROUND THE WORLD



By Anna Paulin, Neha Joy and Shivani Shetty

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

Parliament passes India's Online Gaming Bill, 2025 to combat fraud and money laundering

The parliament passed the "Promotion and Regulation of Online Gaming Bill, 2025" on 21 August 2025. The bill has come into force to fight against addiction, financial loss and social distress. Online money gaming platforms have caused widespread harm, including fraud, money laundering and financial exploitation. Investigations revealed some gaming platforms were used for terror financing and illegal messaging, which poses a threat to national security. Gambling and betting were already restricted in India. But the online domain remained largely unregulated. The bill ensures that both apply in digital and physical places. The bill illustrates the balance between technological innovation and social protection.

Source: [Press Information Bureau](#)

Nepal mandates PSPs to freeze Terrorist linked assets

Nepal's central bank directed payment service providers (PSPs) to freeze assets of individuals and entities designated as terrorists by the UN security council (UNSC) or Nepal's Home Ministry. Until now PSPs verified customers based on their Know your customer (KYC) details. But now they must check if the customer is on the sanctioned list of UNSC or the Nepal Home Ministry. These new guidelines mandate that any terrorist designated party's financial resources direct or indirect be immediately blocked, significantly strengthening AML (anti-money laundering) and CTF (counter-terrorist financing) safeguards. Nepal has 22 licensed PSPs. They must subscribe to the UN sanction list for notifications, and monitor the ministries website regularly. This move is a pivotal step in Nepal's efforts to exit the FATF grey list.

Source: [The Kathmandu Post](#)

AUSTRAC orders Binance to conduct audit over money laundering concerns

Australia's financial crime watchdog Australian Transaction Reports and Analysis Centre (AUSTRAC) has ordered Binance Australia to appoint an external auditor after finding

weaknesses in its anti-money laundering and counter-terrorism financing controls. The regulator cited limited independent review, lack of local staff, and weak senior management oversight at the crypto firm.

AUSTRAC's 2024 National Risk Assessment warns of the rising risk of digital currencies being exploited by criminals. Its chief stressed the need for stronger controls from global crypto firms since this sector handles large transaction volumes.

Source: Reuters

ED busts international drug cartel using Indian mules

The Enforcement Directorate (ED) has launched a multi-state crackdown on an international drug cartel involving Indian nationals acting as mules. The probe was triggered by a Goa Police case earlier this year, when 4.3 kg of cocaine concealed in wafer and coffee packets was seized in South Goa. Investigations revealed that a Zimbabwe national, Tariro Mangwana, remanded to ED custody, played a key role in laundering funds and managing logistics for Indian mules. Out of eight identified Indians, four have already been arrested. The ED's searches in multiple states uncovered evidence of a wider organised syndicate with international links. Investigators found the

use of shell companies, benami accounts, and layering techniques to disguise drug proceeds. The cartel had extensive cross-border contacts for procurement, trafficking, and distribution of narcotics.

Source: [The Indian Express](#)

UAE Central Bank fines exchange house for AML violations

The UAE Central Bank has imposed a Dh2 million fine on Malik Exchange and revoked its licence for failing to comply with anti-money laundering (AML) and counter-terrorism financing regulations. The exchange house's name has also been removed from the official register, as per the laws governing AML and the Combating the Financing of Terrorism and Illegal Organisations. The Central Bank's investigation revealed that Malik Exchange failed to comply with the necessary legal and regulatory requirements.

Source: [Khaleej Times](#)

Two Arrested for cryptocurrency money laundering

Mumbai Crime Branch arrested two individuals for laundering money obtained through cyber fraud by

converting it into cryptocurrency (USDT) and transferring it to Chinese nationals. Preliminary investigations indicate the laundered funds were proceeds of cyber scams targeting Indian citizens, and authorities are probing a larger network misusing Indian bank accounts to convert stolen money into cryptocurrency and transfer it abroad. The Crime Branch continues to trace other accomplices involved in this international money laundering network.

Source: [The Times of India](#)

Europol cracks down Albanian Criminal Network

A Europol-coordinated operation led to the arrests of 10 members of an internationally active Albanian organised crime network, involved in cocaine trafficking and extensive money laundering. Supported by agencies in Albania, Belgium, France, and the Netherlands, authorities seized luxury assets, tourist resorts, villas, apartments, vehicles, and business shares. The kingpin reportedly received over \$40 million from a single shipment, laundering illicit proceeds into real estate and corporate investments across Europe. He coordinated these massive criminal undertakings from remote locations, relying on encrypted

means of communication. Investigations revealed that the network is connected to other high-risk, poly-criminal organisations operating both within the EU and internationally thus leaving a global impact.

Source: Europol

REGULATORY UPDATE



AUSTRALIA NEW AML/CFT REFORMS

By Neha Joy

Australia has taken a major step to strengthen its defences against money laundering, terrorism financing, and serious financial crime through the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Amendment Act 2024. By doing so, Australia is aligning itself with international standards set by the Financial Action Task Force (FATF) and enhancing the integrity of its financial system.

This legislation broadens the scope of AML/CTF regulation to cover new high-risk sectors, known as tranche 2 entities, including real estate professionals, lawyers, accountants, conveyancers, trust and company service providers, and dealers in precious metals and stones. By expanding regulation to previously unregulated but high-risk professions and modernising obligations for existing reporting entities, the government is strengthening its defences against money laundering, terrorism financing, and proliferation financing. The reforms also introduced several specific updates to strengthen enforcement and improve clarity. From March 2025, the tipping-off offence only applies if sharing information could affect an investigation. This gives businesses more freedom to share

information internally without breaching the law. In addition, the Financial Transaction Reports Act 1988 was repealed in January 2025, with all reporting obligations now consolidated under the updated AML/CTF framework.

These reforms represent the most significant transformation of Australia's AML/CTF framework since its inception. By expanding regulation to previously unregulated but high-risk professions and modernising obligations for existing reporting entities, the government is strengthening its defences against money laundering, terrorism financing, and proliferation financing.

Source: AUSTRAC

DOMAIN MATTERS



How to Transition to an Effective Monitoring of Suspicious Activity (MSA) Framework

By Shivani Shetty

The financial crime space has significantly evolved and financial institutions (FIs) need to embrace an innovation framework that allows prompt responses to evolving threats.

According to the Wolfsberg Group, the three core aspects for building a responsible transition framework for innovation in Monitoring of Suspicious Activity (MSA) are:

1. Transition and validation
2. Model risk balanced with financial crime risk
3. Explainability to demonstrate transparency in coverage and effectiveness

The following sections explain how FIs can transition effectively to a new MSA approach that reflects their risk appetite, integrates with broader risk management frameworks, and utilises technology to prevent financial crime.

Define desired outcomes

The transition should begin with establishing clear outcomes in line with the FI's risk appetite and evolving risk management framework. While older systems are based on broad "catch all" mechanisms, a modern MSA framework should complement parallel activities such as enhanced front-office awareness and training on financial crime risks, data analytics capabilities that target specific criminal typologies and financial intelligence units (FIUs) staffed with experienced investigators. The new framework should not aim to replicate the legacy approach but to integrate

seamlessly with these parallel processes, ensuring higher quality outcomes.

Redefine success criteria

In line with the advancements, FIs can redefine the performance indicators to ensure the framework achieves its objectives. Following are some indicators:

- **Priority Risk Coverage:** The model can detect financial crimes tied to high-impact risks as determined by the institution's own threat assessment or national priorities, which are usually not addressed by other controls.
- **Expanded Risk Indicator Coverage:** Incorporate data beyond transactions such as behavioral, network, or contextual data to strengthen detection capabilities.
- **Precision Rate:** The major proportion of alerts are true positives, reducing noise for investigators.

These success criteria should be constantly checked to see if the new approach is minimising overlap in control coverage, optimising new data points beyond transactional data and ensuring complementary processes are in place to facilitate collaboration and coordination.

Transition

The transition from the existing approach to a new approach should be tailored to the desired outcomes of the new approach. Validation and rigorous testing are key steps to ensure the right processes are in place and risks are managed appropriately.

FIs can conduct proof-of-concept exercises in test environments during the transition phase. Modern validation techniques enable performance assessments of new models against historical data, ensuring an appropriate balance between recall and the discovery of emerging risk areas. These evaluations can help determine whether the new model aligns with the updated performance criteria and the FI's defined risk appetite.

FIs also need to prioritise the following during the transition phase:

- Product coverage: Ensure there is clarity on which products, accounts, transaction types are in scope and stakeholders are aware about any limitations.
- Case investigation readiness: FIs should upskill and train investigators with the necessary domain knowledge to handle more complex alerts generated by the system.

Validation

The objective of validation should be that the new framework meets revised success measures and not whether it mirrors legacy outcomes. Institutions can compare SAR quality across old and new approaches and validate whether missed cases are addressed by other controls. FIs should check if productivity is improved by analysing alerts that emerge only under the new system and ensure these are in line with the priority risk coverage and risk indicators.

Apart from the process of transition and validation, audit, assurance and model risk management (MRM) practices also play a role in the pace of production and approval for financial crime models. Lastly, compliance teams must be able to explain the new approach, show how it aligns with revised effectiveness measures, and train analysts to interpret complex monitoring results.

Source: Wolfsberg Group

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