the laundry times

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

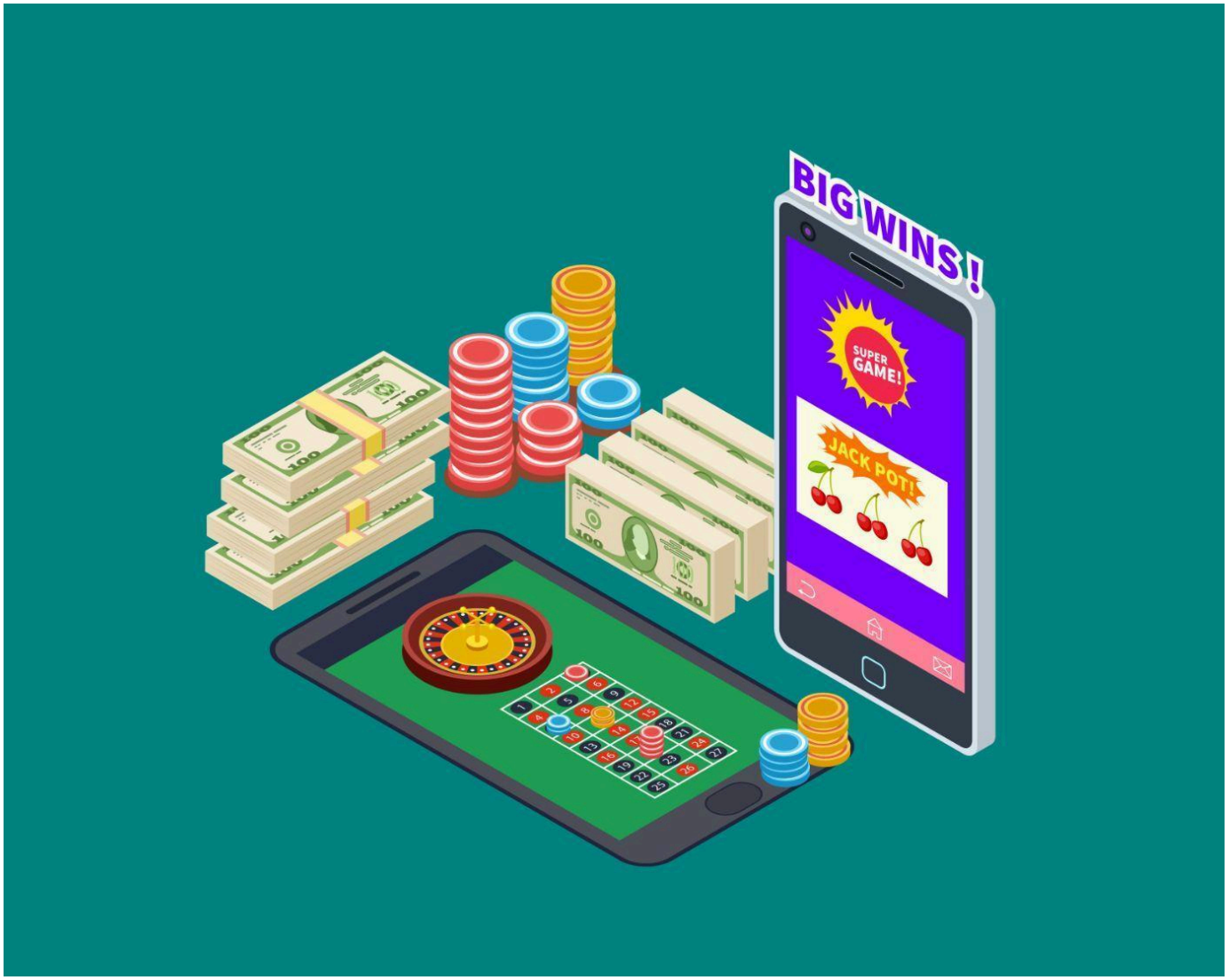
MONTHLY NEWSLETTER

navigate

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

May, 2025

TOP STORY



Fairplay betting app involved in Rs. 13,000 crore money laundering operation

By Shivani Shetty

FairPlay, the betting application, is currently under investigation by the Enforcement Directorate (ED) for its alleged involvement in money laundering. The case came into light following a complaint by Viacom18, which accused several gaming and betting companies including FairPlay of illegally streaming Indian Premier League (IPL) matches, resulting in copyright violations and financial losses.

FairPlay doesn't have a physical presence in India, with no registered entity to conduct its business in the country, nor has it acquired any official documents such as GST number or PAN card for their operations. The online gaming and betting landscape in India is complex and hence the accused strategically moved operations offshore by setting up FairPlay in Curacao, while also forming additional entities in Dubai, Malta, and other regions, thus allowing FairPlay to operate from outside India.

Investigations revealed that FairPlay employed a marketing strategy that included collaborating with high-profile celebrities as brand ambassadors to ensure an image of credibility and mainstream acceptance, which in turn attracted a significant user base.

The ED’s chargesheet has named four companies, Flawless Pharma Pvt Ltd, Aaquries Global Industries Ltd, Remedium Lifecare Ltd, and MEDEC Medicare Ltd through which Rs 4,000 crore was transferred under the guise of importing fictitious or

illegal goods. In total around Rs 13,000 crore is believed to have been funneled abroad through these shell company accounts.

Betty Finserve, a payment gateway played a crucial role by serving as a payout facilitator for FairPlay, enabling the transfer of funds to its clients. Further, Truefund Innovation India acted as an illegal intermediary, managing the funds collected by FairPlay. To further obscure the money trail, the accused allegedly set up a network of dummy, mule, and shell bank accounts to layer and channel funds derived from illegal betting activities.

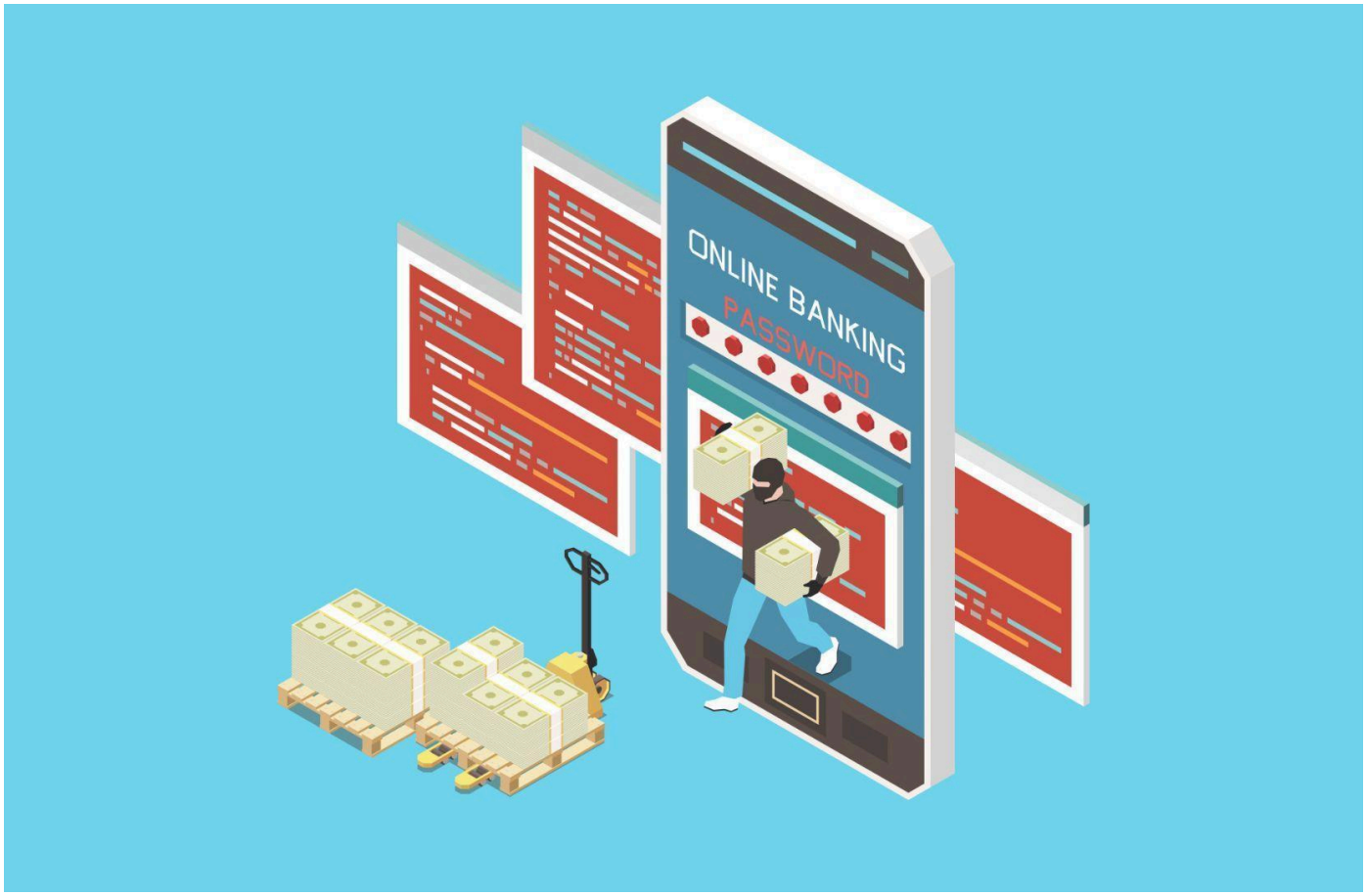
The case highlights the use of a payment gateway as a payout facilitator for illegal activities, and the need for measures to prevent the misuse of such channels. With cases like these coming into light, government officials are increasingly concerned about the significant volumes of unaccounted money circulating within online gaming and betting platforms. Hence, there is a strong push to bring such platforms under the ambit of the Prevention of Money Laundering Act (PMLA). This would require operators to implement compliance programs, including investigating and reporting of suspicious transactions. This could be a critical step towards curbing money laundering and ensuring greater accountability among online gaming and betting companies.

Source: The Economic Times

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]



Cyber fraud racket exposed

A major cyber fraud was recently uncovered in Mumbai revealing a massive cyber fraud racket that exploited job seekers to create fake bank accounts used in large scale money laundering.The case came into light when a 20 year old woman, received an unexpected Income Tax notice demanding payment for unreported cash deposit totalling to Rs.5 crores. Upon further investigation, it was found that she had previously submitted her personal details and documents to individuals who had promised her job. These documents were used by the criminals to open multiple bank accounts to launder money obtained through scams impersonating government or bank officials. The criminal group lured employees with fake job offers and collected their Aadhar, PAN and other documents and used them to create multiple mule accounts. The case highlights the importance of safeguarding personal information and being cautious when sharing personal documents.

Source: Hindustan Times

Police uncover 7,200 mule accounts linked to cybercrime and money laundering

In 2025, J&K Police identified over 7,200 mule accounts used for laundering money obtained through cyber fraud, and estimates suggest that the total number could be 30,000. These accounts, involving individuals, shell companies, or enterprises, are often remotely controlled by fraudsters based outside J&K or even

overseas. The transaction volumes linked to these accounts are in crores and once activated, the accounts are used to rapidly move funds to other accounts or convert them into cryptocurrency. So far, 19 arrests have been made, and investigations are ongoing.

Source: The Times of India

FIU and RBI sign MoU for enhanced co-ordination and information exchange

The Financial Intelligence Unit (FIU) - India and the Reserve Bank of India (RBI) have signed a Memorandum of Understanding (MoU) to enhance their efforts in combating money laundering. The agreement aims to strengthen cooperation and sharing of information between the two entities. The collaboration will help in the upgradation of Anti-Money Laundering/ combating financing of terrorism (AML/CFT) skills in regulated entities. The MoU will also help in identification of red flag indicators for suspicious transactions. The MoU signifies a strategic move to strengthen India's financial institutions against money laundering and terrorist financing threats with the help of inter-agency cooperation.

Source: PIB

Nepal discusses action plan to exit FATF Grey list

Financial Action Task Force (FATF) FATF recently placed Nepal on its grey list for the second time due to deficiencies in combating money laundering and terrorist financing. In an effort to meet global standards, the Nepal government has now finalized an action plan with clear responsibilities and deadlines to address these gaps within two years to avoid being placed in the black list and face harsher sanctions. During a meeting of the Anti Money Laundering Prevention Directorate Committee on 8th April, the Finance Minister Bishnu Prasad Paudel stressed the need for a long-term strategy to prevent future relisting. Officials also stated the importance of institutional governance, inter-agency coordination, and technology. The meeting discussed the need for Nepal to focus on risk assessment, investigation and prosecution, with implementation being prioritized over legal changes.

Source: The Kathmandu Post

2 Nigerians, among 3 held in Hyderabad for money laundering and drug trade

Telangana Police arrested two Nigerian nationals, Ugwu Ikechukwu and Chukwu Ogbonna, along with forex agent Mohammed Mateen, for their involvement in an international drug and money laundering network. The police seized drugs, ₹45,000 in cash, and other incriminating materials linked to their operation in Hyderabad, Bangalore, and the US. The modus operandi

involved targeting single women in the US, from whom Ikechukwu fraudulently obtained bank and credit card details. These were provided to US-based drug buyers to make payments. To launder the money, Mateen, through Anand Jain of Goyam Forex, sourced US-based Indian bank accounts. The women transferred funds via money transfer services into these accounts, and Mateen handed over cash to the fraudsters in India.

Source: The Indian Express

Eight arrested in Hong Kong for identity theft through deepfake technology

Hong Kong police arrested eight individuals linked to a fraud ring that used deepfake technology to bypass banks' identity verification systems. The group used artificial intelligence to merge their own facial features with photos from lost or stolen identity cards, creating hyper-realistic fake images. These manipulated visuals were then used in online banking applications to impersonate the actual ID holders. This incident highlights the growing risk from the use of AI by fraudsters, especially as financial institutions shift towards digital channels.

Source: South China Morning Post

REGULATORY UPDATE

Indian Cybercrime Coordination Centre (I4C) empowered under PMLA

By Anna Paulin

The Ministry of Home Affairs (MHA) has established the Indian Cybercrime Coordination Centre (ICCC), also known as I4C, as the central agency for tackling cybercrime in a coordinated and comprehensive way. The Revenue Department under the Finance Ministry included I4C under Section 66 of the Prevention of Money Laundering Act (PMLA 2002). I4C has been authorised to share and receive information from the Enforcement Directorate under the anti-money laundering law.

While this would facilitate I4C to share and receive information from the Enforcement Directorate and further help in coordination, it would not have any direct authority to prosecute under the PMLA. Through information sharing with I4C, it would help in tracing money trails and uncovering the transnational masterminds behind cyber frauds.

This initiative is a significant step towards combating online financial crimes and addressing the growing issue of cyber fraud within the banking system, online gaming, and betting companies.

Source: The Economic Times

DOMAIN MATTERS

API Misuse and BC-Driven Money Laundering

By Neha Joy

Business Correspondents (BCs) are appointed by banks to provide basic banking services in rural and underserved areas. However, some of these BCs have been found misusing their privileges. By impersonating as merchants or small businesses, they access bank payout APIs originally intended for salary payouts, vendor

payments, and refunds. These APIs are then used to channel illicit cash collections into the formal banking system.

The money travels through a string of agents who collect cash from faceless individuals who do not reveal their source of money. The cash received is then deposited in a bank account by the BC. Subsequently, the BC leverages the API of a partnered payment aggregator (PA) to transfer these funds, often in varying amounts, from their account to numerous beneficiary accounts. The process involves the money initially moving from the BC's account to the PA's account before reaching the final beneficiaries. This entire mechanism depends on the BC falsely presenting themselves as a merchant, establishing an agreement with the PA, and disguising each money transfer as a transaction between two merchants.

The core issue lies in insufficient due diligence by some payment aggregators while onboarding merchants. Many fintech platforms allow near-instant onboarding, often with relaxed Know Your Customer (KYC) practices or insufficient verification of business legitimacy. This opens up a vulnerability that fraudsters are exploiting. Furthermore, the payments industry is working toward developing a centralized fraud repository, a database of known fraudulent entities, rogue merchants, and compromised accounts. This will allow payment gateways to share intelligence and flag suspicious actors before they can move to another platform.

The Reserve Bank of India (RBI) has issued draft guidelines aimed at tightening the operations of payment aggregators. The misuse of bank payout APIs to route illicit funds has prompted the RBI to propose stricter Know Your Customer (KYC) and merchant onboarding norms. These include video-based KYC, verification of business legitimacy, and enhanced due diligence for high-risk

merchants.The guidelines also call for real-time transaction monitoring to detect suspicious patterns, along with mandatory tagging of transaction purposes and regular reporting to the Financial Intelligence Unit (FIU). To stop people from misusing the payout APIs, access will be restricted to entities with strong compliance records.

The RBI proposes clearer accountability among payment aggregators, banks, and merchants, with penalties for violations such as license suspension or blacklisting. Outsourcing of core functions like KYC and transaction monitoring will require prior approval, ensuring agents like business correspondents adhere to the same standards. Additionally, the industry is planning to introduce a centralized negative database, an information-sharing platform that will list known fraudsters and suspicious merchants. This will help prevent bad actors from hopping between platforms once they are flagged.

Source: The Economic Times

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