# 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

June, 2025

# TOP STORY

## RBI Annual Report 2024-25: Highlights on Financial Frauds

By Neha Joy

The Reserve Bank of India's (RBI) Annual Report for 2024–25 reveals a decrease in the number of banking frauds with a significant increase in the amount involved.

During FY25, 23,953 cases were reported compared to 36,060 in the previous year. Frauds have occurred predominantly in the category of digital payments.

The rise in the total amount involved in frauds in 2024–25 compared to 2023–24 was primarily due to the removal of fraud classification in 122 cases amounting to ₹18,674 crore which was later reported again following a reassessment in line with the Supreme Court's March 27, 2023, ruling. An analysis of fraud cases by bank groups over the past three years shows that private sector banks recorded the highest number of fraud incidents, while public sector banks accounted for the largest share in terms of the total value involved.

The report highlights the changing dynamics of banking frauds in India, with a notable shift towards digital platforms. Continued investment in cybersecurity and regulatory oversight will be key to safeguarding the financial system from emerging threats. The Reserve Bank undertook several measures to safeguard the financial system by further strengthening the regulatory and supervisory framework of banking and non-banking sectors in line with global best practices.

Source: RBI

# 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]

## STRs submitted in Nepal surge by 49% as compared to previous year

According to the fourth annual newsletter released by Nepal Rastra Bank, there was a 49% increase in Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) submitted by reporting institutions in 2024 compared to 2023. FIU-Nepal received 9,304 STRs in 2024, which is the highest since the enactment of the Money Laundering Prevention Act, 2008. Threshold Transaction Reports (TTRs) also rose to 1.97 million from 1.78 million in 2023. The majority of STRs originated from commercial banks, followed by development banks, finance companies, and stock brokers. The FIU also expanded its goAML system, connecting 1,905 entities, including newly onboarded Designated Non-Financial Businesses and Professions (DNFBPs) such as casinos and real estate agents.

Source: The Rising Nepal

# Multimillion Euro investment scam dismantled

Europol has successfully dismantled a sophisticated multimillion-euro investment scam that defrauded thousands of victims across Europe. The fraudulent scheme, orchestrated by an organized crime group, promised high returns through investments in cryptocurrency-related products, including leasing and subleasing of crypto exchange machines and cloud server storage. However, investigations revealed that the advertised equipment and systems were non-existent, and the operation functioned as a classic pyramid scheme. This operation was part

of a broader effort by European authorities to combat online investment fraud.

Source: Europol

# Police uncover gambling ring using AI for money laundering

Vietnamese Police in Thái Bình province are investigating 21 individuals involved in a major transnational gambling and money laundering ring. The group was operating through the foreign-based website 'KUBET' and used artificial intelligence (AI) to facilitate and conceal illegal activities. Over one million gambling accounts placed bets totaling over US$ 39.2 million. The ring's Taiwanese ringleader had domestic accomplices who used AI-generated videos to bypass biometric banking verification and launder funds through multiple Vietnamese bank accounts. Monthly laundering exceeded VNĐ200 billion (US$7.84 million), with over VNĐ1 trillion laundered between September 2024 and April 2025. Police have frozen more than 500 bank accounts and continue to investigate the large-scale criminal network.

Source: Việt Nam News

# ₹11,500 crore diverted through shell companies

The Enforcement Directorate (ED) has uncovered a financial fraud involving Dewan Housing Finance Corporation Limited (DHFL). Former promoters Kapil and Dheeraj Wadhawan allegedly diverted over ₹11,500 crore through 87 shell companies set up in the names of associates and employees. These entities had no real operations and were used to siphon off money. A fake branch was created through which 2.6 lakhs fake home loan accounts were generated without undergoing standard verification. The funds were reportedly used to purchase luxury goods. The ED has registered a formal case and is conducting a thorough investigation into the matter.

Source: Hindustan Times

# Swiss Bank Julius Baer fined for AML compliance failures

Swiss private bank Julius Baer has been ordered by the country's financial regulator, FINMA, to pay over $4.8 million for non-compliance with anti-money laundering regulations. According to FINMA, the violations occurred between 2009 and 2019 and involved significant compliance failures. The regulator's investigation found that the bank failed to take necessary action in response to suspicious transactions involving high-risk clients and continued managing their accounts despite clear red flags.

Source: Reuters

# Online fraud gang with international link busted

The Jaipur Crime Branch recently uncovered a cyber fraud ring with suspected links to China, arresting six individuals including the gang leader. Operating from a hotel in Narayan Vihar, Mansarovar, the group facilitated money laundering by purchasing Indian bank accounts from locals at a lower commission and reselling them to Chinese operators of fraudulent online trading and gaming platforms at high percentage, using encrypted platforms like Telegram. A case has been registered, and investigations are ongoing into the network's wider international links.

Source: The Times of India

# Digital arrest scam: ₹1.82 crore fraud exposed

Navi Mumbai police busted an international cybercrime gang involved in digital arrest scams after a medical college professor was defrauded of ₹1.82 crore. The fraudsters contacted her through WhatsApp video call, posing as Income Tax officials, and falsely accused her of tax evasion and money laundering. Using forged documents with logos of the CBI, ED, and Supreme Court, they convinced her to transfer money into different accounts for supposed RBI verification. Between January 14 and February 15,

the woman transferred a total of ₹1.82 crore to six different bank accounts using the details shared by the scammers. The investigation is still underway to uncover more details about the case.

Source: Hindustan Times

---

# TECH TRENDS

## DoT introduces Financial Fraud Risk Indicator (FRI) to reduce cyber fraud

By Shivani Shetty


The Department of Telecommunications (DoT) has introduced the Financial Fraud Risk Indicator (FRI) with key stakeholders as an integral move to reduce financial crime. This indicator is the result of a multi-dimensional analytical tool developed as part of the Digital Intelligence Platform (DIP), aimed at aiding banks, UPI service providers and other financial institutions with enhanced intelligence for preventing cyber fraud.

The FRI is a risk-based metric that categorizes mobile numbers into Medium, High, or Very High risk of financial fraud. This classification is derived from inputs provided by multiple sources such as reporting from Indian Cybercrime Coordination Centre (I4C)'s National Cybercrime Reporting Portal (NCRP) and intelligence from banks and financial institutions.

The Financial Fraud Risk Indicator (FRI) works as soon as a suspected mobile number is flagged by a stakeholder. The number goes through multidimensional analysis and is assigned a risk category, which is instantly shared with all stakeholders via the DoT's Digital Intelligence Platform (DIP).

The DoT's intelligence unit also regularly provides a list of disconnected mobile numbers, along with reasons such as involvement in cybercrime, failed re-verification, or exceeding usage limits, factors often linked to financial fraud. Since these numbers are usually used for only a few days, and full verification takes time, the FRI serves as an advanced indicator of risk.

Widely used UPI platforms in India such as Google Pay, PhonePe and PayTM have begun integrating DIP alerts into their system. PhonePe, an initial adopter of FRI, has used it to decline transactions linked to Very High FRI mobile numbers and display an on-screen alert. The data shared by PhonePe indicates the effectiveness of the FRI model, as there is a high correlation between flagged numbers and confirmed cyber fraud cases.

There has been a rise in the issuing of “ghost” phone numbers by cyber fraudsters used to deceive people online through tactics like investment scams, digital arrests and impersonation. These illicit numbers are further used to open fraudulent bank accounts and make deceptive calls to unsuspecting victims. To tackle this growing issue, FRI enables real-time validation checks when a digital payment is initiated to a flagged number. It facilitates swift, targeted, and collaborative responses across the telecom and financial sectors. With UPI being the dominant payment method in India, this timely intervention could protect millions of citizens from cyber fraud.

Source: PIB

---

# DOMAIN MATTERS

## How to implement a Risk Based Approach (RBA)

By Anna Paulin


According to FATF Recommendation 1, the Risk-Based Approach requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks they face and to implement measures that mitigate those risks appropriately. The general principle is that entities should

apply enhanced measures in high-risk areas, while lower-risk scenarios may be managed with simplified procedures.

Assessing the nature of risk is essential as both governments and private sector entities are expected to conduct risk assessments, such as National Risk Assessments (NRAs) at the country level or internal risk assessments within institutions.  On an institutional level, firms must evaluate risks based on customers, geographic exposure, products and services offered, and delivery channels. This helps detect areas susceptible to misuse, such as high-risk sectors or jurisdictions with weak AML/CFT controls.

Once risks are identified, institutions must take proportionate action to mitigate these risks. Higher-risk customers or transactions should undergo enhanced due diligence measures, such as more rigorous identity verification and closer monitoring of account activity. On the other hand, in cases where the risk is relatively low, institutions may apply simplified due diligence procedures to reduce the regulatory burden while still adhering to compliance requirements.

Financial institutions and DBFBPs are required to establish and maintain policies, controls and procedures tailored to their risk profiles. The adoption of appropriate technology such as transaction monitoring systems, artificial intelligence and analytical tools can further enhance the accuracy of risk assessment.

Lastly, risk profiles are not static as they evolve over time due to changes in the regulations, geopolitical developments, or new technologies. Staff must be equipped to recognize evolving risk indicators and understand due diligence obligations. A robust RBA is not a one-time process; it necessitates ongoing monitoring. Hence, institutions must regularly review and update their risk based approach to ensure it remains effective and responsive to the changing financial crime domain.

---

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