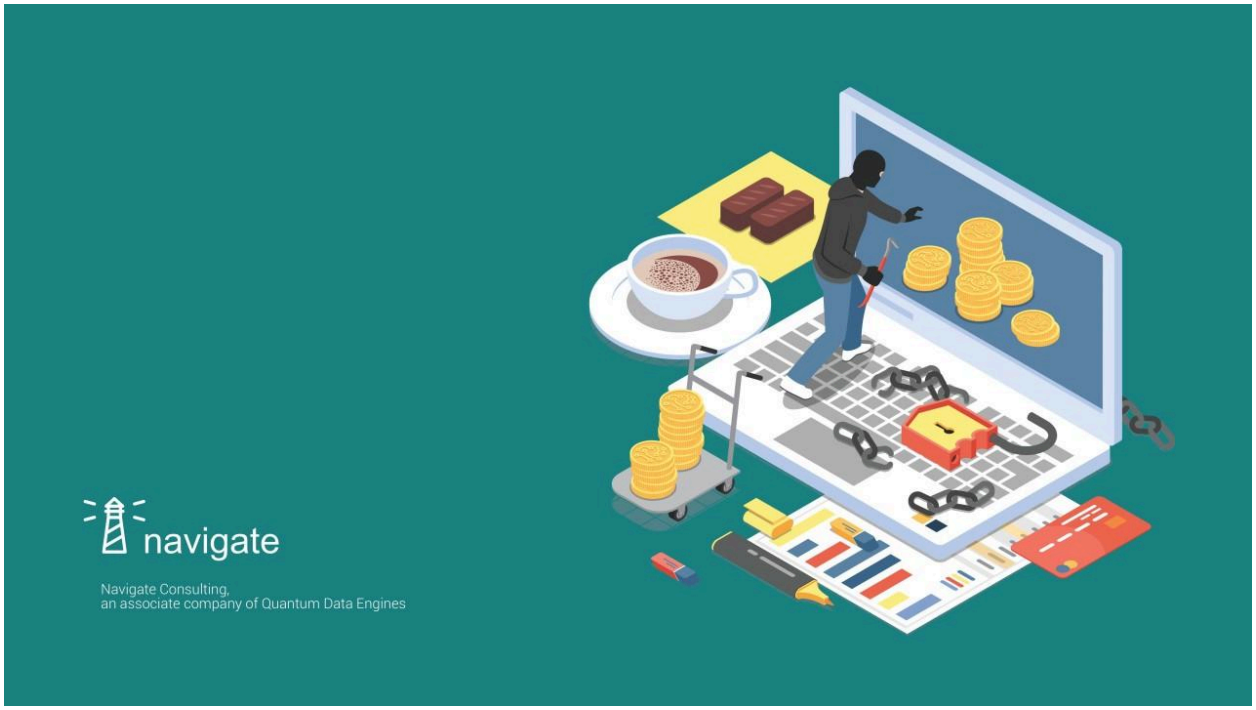


FATF on Cyber-Enabled Fraud | Emerging Money Laundering Trends in Nepal | FinCEN updates CDD requirements and more

March 6, 2026

FATF on Cyber-Enabled Fraud as a Growing Global Risk

By Neha Treesa Joy

Financial infrastructure developments have significantly increased the complexity of combating cyber-enabled fraud. The rapid expansion of virtual assets, instant payment systems, and cross-border financial channels has transformed the speed at which funds can move across jurisdictions. While these innovations enhance efficiency and financial

inclusion, they also create opportunities for criminals to transfer illicit proceeds before detection or intervention is possible.

Over the last few years, the Financial Action Task Force (FATF) has recommended the following steps, which can assist countries and financial institutions in tracing and preventing the generation and transfer of fraud proceeds:

- Payment Transparency: Improving payment transparency is essential to mitigate risks arising from cyber-enabled fraud. It highlights the importance of ensuring that accurate originator and beneficiary information accompanies wire transfers and other payment messages so that competent authorities and financial institutions can trace transactions and identify suspicious activity more effectively.
- Unmasking Beneficial Ownership: Revised beneficial ownership standards mandate a risk-based, multi-pronged approach to collecting and using ownership information to prevent misuse of shell companies. Accurate, up-to-date, and accessible beneficial ownership data enables authorities to identify the natural persons who ultimately control legal entities involved in fraud schemes.
- Regulation of Virtual Assets: Since 2019, FATF standards recommend the regulation of Virtual Asset Service Providers (VASPs) with AML/CFT obligations, such as customer due diligence and transaction monitoring. This also includes the implementation of the Travel Rule, which involves the transmission of originator and beneficiary information in virtual asset transfers.
- Employing Advanced Technology: Machine learning models, real-time payment risk scoring, and anomaly detection systems are increasingly deployed to identify suspicious patterns at scale. These tools help institutions process vast transaction volumes and flag high-risk behaviour that would not be detectable through manual review alone.
- Asset Recovery Standards: Jurisdictions need to have effective mechanisms to freeze, seize and confiscate proceeds of crime. Rapid action is critical in cyber-enabled

fraud cases due to the speed at which funds can be transferred across accounts and borders, and it underlines the importance of international cooperation in tracing and recovering assets.

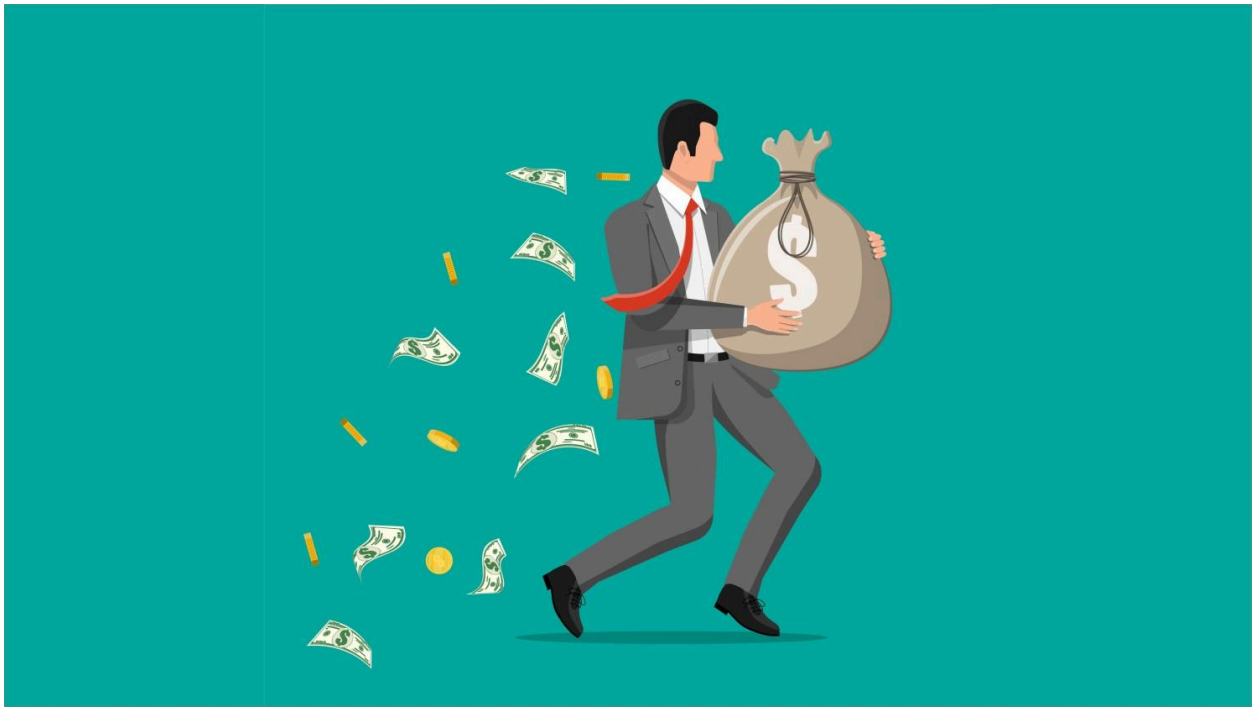
- Domestic and International Partnerships: Information sharing between financial institutions, financial intelligence units (FIUs), law enforcement, and international counterparts is critical to disrupting fraud networks operating in real time. Public-private partnerships facilitate the rapid exchange of typologies, red-flag indicators, and emerging scam methodologies.

Cyber-enabled fraud has evolved into a systemic financial crime risk that intersects directly with money laundering, terrorist financing, and proliferation financing. As digital payments, virtual assets, and cross-border financial services continue to expand, so does the opportunity for criminals to exploit speed, scale, and anonymity. Effective implementation of advanced technology, real-time information sharing, and sustained international coordination are essential to disrupt fraud networks and recover illicit proceeds.

Source: FATF

NEWS SNIPS FROM AROUND THE WORLD

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



₹7 crore digital arrest and money laundering case

The Enforcement Directorate (ED) has filed a prosecution complaint in a money-laundering case linked to the digital arrest case of Ludhiana industrialist S. P. Oswal. The probe found that cybercrime proceeds, including ₹7 crore from the digital arrest, were routed through mule accounts. The accused reportedly provided mule bank accounts to individuals based in Cambodia and Vietnam and received commissions in the form of cryptocurrency. The stolen money was then transferred systematically through multiple mule accounts to conceal the source of the funds. Part of the money was layered through shell entities and sent outside India using trade-based money laundering methods. The remaining funds were distributed in smaller amounts ranging

from ₹2–₹5 lakh across several mule accounts, from which cash was immediately withdrawn. This cash was later used to purchase virtual digital assets, which were transferred to accounts of foreign nationals after deducting commission.

Source: The Times of India

Two arrested in Rs. 2.88 crore investment scam

Mumbai Police arrested two men for allegedly cheating a textile trader of ₹2.88 crore by promising fixed monthly returns of 5% on an investment scheme. The accused allegedly used a company to project a legitimate business opportunity and persuaded the victim to transfer funds through multiple bank transactions. The victim transferred Rs. 2.88 crore in six RTGS transactions to the company's account. After collecting the money, they failed to deliver the promised returns and eventually became unreachable. Police investigations suggest the scheme was fraudulent from the outset, with misleading claims about company operations and roles, and that portions of the funds were diverted to various accounts.

Source: The Indian Express

FinCEN updates Customer Due Diligence (CDD) requirements

The Financial Crimes Enforcement Network (FinCEN) has issued an order that grants exceptive relief for financial institutions from the requirement to identify and verify beneficial owners of a legal entity customer each time the customer opens a new account. According to this order, covered financial institutions are only required to confirm beneficial ownership when the business first opens an account, when there is cause to doubt the authenticity of the information already acquired, or when their risk-based procedures for ongoing due diligence demand it. The Bank Secrecy Act's other

anti-money laundering obligations, such as ongoing monitoring and reporting of suspicious transactions, remain the same.

Source: FinCEN

Student bank account used to route ₹7 crore

A 23-year-old engineering student was arrested after his bank account was allegedly used to route nearly ₹7 crore as part of a cybercrime network. Investigators believe that he was involved in facilitating mule account operations that enabled fraudulent transactions across states. The case came to light when the student approached the police after his bank account was frozen. Transactions worth about ₹ 7 crore had been processed through his account within 48 hours. According to the student, he shared his passbook, ATM card, SIM card and other banking details with a friend who allegedly misused them.

Source: The Times of India

EMERGING TRENDS

Emerging Money Laundering (ML) Trends in Nepal

By Adhila Thirumalai

Money laundering in Nepal is becoming more structured, technologically driven, and interconnected with cross-border systems, according to the Financial Intelligence Unit (FIU) - Nepal FY 2024-25 report.

Following are the emerging ML trends in Nepal:

- Trade-Based Money Laundering (TBML): TBML-related STRs filed rose from 22 in FY 2023-24 to 43 in FY 2024-25. The report highlights the increasing risks from phantom

shipments, misdescription of goods, under-invoicing, over-invoicing, split invoicing, overshipment and shell companies.

- Predicate Offences: In Nepal, while predicate offence categories such as money laundering, tax-related, fraud, money and banking continue to remain the most reported categories, the country is witnessing new reported categories, including Hundi, Virtual Currency, and Undue Transactions that appeared for the first time in FY 2024-25.
- Hundi through Cryptocurrency: A structuring typology has been observed in which large volumes of cash are deposited in an account by multiple unrelated third parties. The funds are then rapidly transferred to various counterparties, often within the same or next day, indicating layering behaviour consistent with informal value transfer systems such as hundi. The use of third-party deposits, the participation of numerous people, and the potential integration of cryptocurrency for settlement purposes point to a coordinated mechanism designed to transfer and settle money outside of official remittance systems while preserving the appearance of legitimacy within the financial system.
- Misuse of Payment Service Providers (PSPs): PSPs are licensed to facilitate digital payments and are not expected to conduct frequent or large-scale cash transactions. However, PSP operational and settlement accounts are being misused for high-value, high-frequency cash deposits that are inconsistent with their intended digital payment model. Funds are rapidly transferred through intermediary and settlement accounts, with vague transaction narratives and repeated involvement of common beneficiaries and entities, indicating layering across multiple institutions.

Thus, emerging ML trends in Nepal emphasise the need to prioritise high-risk STRs/SARs for immediate and proactive analysis. Financial institutions must strengthen their ability to uncover hidden networks and complex transaction patterns that are difficult to detect through manual review alone. This can be done through the implementation of a robust risk-based approach, enhanced screening and monitoring systems, and stronger analytical capabilities.

Source: Nepal FIU Annual Report 2024-25

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.