STORIES THIS MONTH
March, 2025

TOP STORY

Operation Thunder and the overlooked side of wildlife crime

by Anna Paulin

INTERPOL and the World Customs coordinated ‘Operation Thunder 2024’ which led to the seizure of nearly 20,000 live animals and the arrest of 365 suspects involved in wildlife and forestry trafficking across 138 countries. In addition to wildlife trafficking, the operation discovered large-scale trafficking of animal parts, plants, endangered species and identified six transnational criminal networks.

Illegal Wildlife Trade (IWT) undermines international conservation efforts and endangers innumerable species. It also fosters corruption, destabilizes economies, and threatens global security. IWT is a global threat, and it thrives on complex fraud and tax evasion. Operation Thunder highlights the significant financial gains associated with wildlife

trafficking, which often necessitate money laundering to integrate illicit profits into the legitimate economy. Criminal networks exploit various methods to launder money, including the use of shell companies, placement and layering of funds, money value transfer systems like Hawala and investment in real estate and luxury goods. The operation also exposed how traffickers leverage social media by creating multiple profiles and linked accounts to increase their reach.

Despite the scale of this crime, financial investigations remain insufficient in many countries, allowing traffickers to perceive IWT as a low-risk, high-reward enterprise. To strengthen the fight against wildlife crime, “INTERPOL has issued Red notices” for 21 internationally wanted traffickers.

Most often criminals involved in IWT are found to be involved in broader criminal activities. Therefore, there is a need for financial institutions to identify red flags, detect suspicious transactions and disrupt financial flows related to wildlife trafficking.

Source: INTERPOL

NEWS SNIPS FROM AROUND THE WORLD

By Shivani Shetty, Anna Paulin and Neha Joy

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

NPCI warns about rise in call merging scams

National Payment Council of India (NPCI) has warned about the Call Merging scam, a new cyber fraud that deceives people into losing money through phone calls. With the help of the merge feature in phone calls, scammers are tricking people into unknowingly sharing their OTP, which enables fraudulent transactions. The scammer manipulates the user into merging the call with an unknown number, claiming it's their friend, which allows unauthorised transactions to take place. The scam also exposed how fraudsters are making use of a basic feature in phones like “call merging” and victims don't suspect any foul play. NPCI has advised precautions like verifying caller identity and avoiding merging calls with unknown numbers to address this threat.

Source: Times of India

FINRA fines Young America Capital for AML program deficiencies

Young America Capital LLC has been fined $50,000 as part of a settlement with the Financial Industry Regulatory Authority (FINRA) for failing to implement an adequate anti-money laundering (AML) program. Since August 2020, the firm has not established proper policies and procedures to detect and report suspicious transactions. Additionally, it failed to provide sufficient AML training to its registered representatives, violating several FINRA rules. The firm, a FINRA member since 2010, has also agreed that a senior management member shall certify that the firm has remediated the deficiencies and implemented a compliant supervisory framework.

Source: FINRA

Philippines exits global watchdog FATF grey list

The Financial Action Task Force (FATF) has removed the Philippines from its ‘grey’ list, which includes countries under increased monitoring for anti-money laundering and counter-terrorism financing deficiencies. This decision was taken after an on-site visit that acknowledged the country's progress in addressing these issues since being placed on the list in June 2021. However, the FATF has urged the Philippines to sustain these improvements and continue working with the Asia/Pacific Group on Money Laundering (APG). Meanwhile, Nepal and Laos have been added to the grey list, bringing the total number of countries on it to 25. The grey list includes nations with strategic financial system deficiencies but that remain committed to resolving them. Countries on this list must implement an action plan within a set timeframe.

Source: The Economic Times

INTERPOL and African Development Bank Join Forces to Combat Financial Crime

INTERPOL (International Criminal Police Organisation) and the African Development Bank (AfDB) have signed a letter of intent to strengthen the fight against financial crime and corruption across Africa. AfDB is the first multilateral development bank to form this kind of partnership with INTERPOL. Currently, the financial magnitude of illicit financial flows in Africa is USD 90 billion annually. This collaboration aims to enhance law enforcement capabilities, promote intelligence sharing, and develop preventive measures against emerging financial crime. With the growing concern about online fraud and financial crime in Africa, this initiative will help nations combat money laundering, fraud, and corruption more effectively.

Source: INTERPOL

RBI introduces AFA for international online payments

The Reserve Bank of India (RBI) plans to enhance the security of international online transactions by introducing an Additional Factor of Authentication (AFA) for cross-border 'Card Not Present' (CNP) transactions. This measure aims to align the security standards of international digital transactions with those of domestic ones. This initiative will help Indian consumers with enhanced protection against cyber threats during international online purchases. AFA adds an extra step to the verification process such as One Time Password (OTP) or biometric authentication to the transaction process. RBI's initiative to introduce AFA underscores its commitment to strengthening the security framework of digital transactions.

Source: Business Standard

ED Uncovers Money Laundering Web in QFX Trade Ltd Probe

The Enforcement Directorate (ED) has frozen over 30 bank accounts holding approximately ₹170 crore, linked to shell companies associated with QFX Trade Ltd. The investigation, initiated based on multiple FIRs filed by Himachal Pradesh Police, revealed that QFX and its agents promoted an unregulated deposit scheme promising investors a 5% monthly return. The ED discovered that QFX Trade Ltd funnelled illicit funds through multiple shell companies and these companies had minimal or no legitimate business operations and were used solely to park and circulate investor funds. Additionally, layering

techniques were employed, with money being circulated through multiple bank accounts, digital wallets, and payment gateways to complicate tracing. As investigations continue, further legal actions against those involved are expected, reinforcing the government's commitment to tackling financial fraud and safeguarding economic integrity.

Source: The Economic Times

The Expanding Human Trafficking Crisis in Myanmar

Over 6,000 individuals from 21 countries are trapped in Myanmar's human trafficking networks, facing torture and forced labour. Many were lured by fake job offers, only to be forced into cyber scams, online fraud, or illegal labour. Criminal syndicates, often linked to armed groups, operate trafficking hubs where victims endure torture, electrocution, and starvation. Some are held for ransom, while others are threatened with organ harvesting or forced marriages. The Civil Society Network and representatives from nine nations have called for urgent action to rescue the victims.

Source: Nation Thailand

New India Cooperative Bank fraud involving Rs. 122 crores

The fraud involved the systematic siphoning of Rs 122 crore from a bank's safes over six years (2019–2025). Hitesh Mehta, a bank general manager, allegedly embezzled the funds and routed them through a developer's company. The fraud was uncovered during an RBI inspection, which revealed cash discrepancies of Rs 112 crore missing from the Prabhadevi branch safe and Rs 10 crore from the Goregaon branch safe. Investigations revealed that part of the stolen funds was sent abroad via hawala channels and deposited into two trusts. This is an ongoing investigation, with several individuals being accused of transfer of illicit funds.

Source: The Indian Express

REGULATORY UPDATE

Exclusive domains announced by RBI to enhance cybersecurity in Indian banking

By Neha Joy

The Reserve Bank of India (RBI) has launched two exclusive website domains to improve cybersecurity in the financial sector. Banks will use the ‘bank.in’ domain, while non-banking financial companies (NBFCs) will use ‘fin.in.’ This initiative aims to create a secure online space for financial institutions, making it easier for customers to identify genuine websites. By doing so, RBI hopes to reduce online fraud, such as phishing attacks, where fake websites are used to trick people into sharing sensitive information. This move is expected to strengthen trust in digital banking and financial services across India. The exclusive domains will help financial institutions establish a verified and uniform digital presence, minimizing the risk of impersonation by fraudulent entities. Additionally, the RBI is expected to implement strict verification processes for domain registrations, ensuring only legitimate banks and NBFCs can acquire these domains.

The Institute for Development and Research in Banking Technology (IDRBT) has been designated as the exclusive registrar for these domains. Registrations for 'bank.in' are set to commence in April 2025, followed by the introduction of 'fin.in' for non-bank financial entities. RBI may also collaborate with cybersecurity experts and law enforcement

agencies to monitor and prevent misuse of these domains, further strengthening the security framework.

By introducing these exclusive domains and additional security measures, RBI aims to strengthen the digital financial infrastructure, protect consumers, and foster greater trust in financial institutions.

Source: The Economic Times

DOMAIN MATTERS

The Role of Front and Shell Companies in laundering proceeds from Environmental Crimes

by Shivani Shetty

The Financial Action Task Force (FATF) provides a strong framework for both countries and the private sector to combat money laundering linked to environmental crimes. As per FATF Recommendation 3, countries are required to criminalize money laundering for a range of environmental offenses, including illegal mining, logging, and waste trafficking. FATF standards also stress on the identification and assessment of money laundering and terrorist financing risks across crime areas, requiring countries to take proactive steps to

mitigate these risks. Criminals use specialised networks for environmental crimes, making it essential to understand how front and shell companies are used to move illicit funds and conceal illegal activities.

Criminals engaged in illegal mining and logging frequently rely on front companies to conceal payments and launder illicit funds. These companies are often located in offshore centers, and work with intermediaries like lawyers and refiners to engage in third-party transactions, creating layers that cover money trails.

One common tactic is mixing illicit proceeds from illegal mining, logging, and waste trafficking with legitimate business accounts. Many of these front companies appear to operate in natural resource sectors, such as mining and forestry, making it difficult to differentiate legal from illegal activities. These businesses typically handle high volumes of transactions with low individual profit margins, making them harder to detect by law enforcement agencies and the financial sector.

In some cases, criminals also use front companies in cash-intensive sectors unrelated to natural resources, particularly import-export businesses. These companies generate fake invoices and supplier payments, creating the illusion of legitimate trade activity.

Beyond front companies, shell companies play a significant role in disguising the true owners behind illegal mining operations. Shell companies located overseas are used to move funds back and forth under the guise of invoices for processing mining business. These companies often have no real business activities and exist solely to facilitate financial transactions linked to illicit activities.

These schemes highlight the critical role of financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) in combatting money laundering linked to environmental crimes. These institutions often lack red flag indicators, training, and typologies to identify illicit financial flows from illegal mining, logging, and waste trafficking.

According to FATF recommendations, financial institutions and DNFBPs must implement AML/CFT measures, including customer due diligence (CDD), record-keeping, and reporting suspicious transactions. These obligations help mitigate risks associated with environmental crime and provide crucial information to law enforcement agencies.

To combat money laundering from environmental crime, institutions must prioritize beneficial ownership transparency and enhanced due diligence, especially for politically exposed persons (PEPs). By improving monitoring systems, regulatory compliance, and international collaboration, financial institutions can help disrupt illicit financial networks that lead to environmental crimes.

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