the laundry times

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

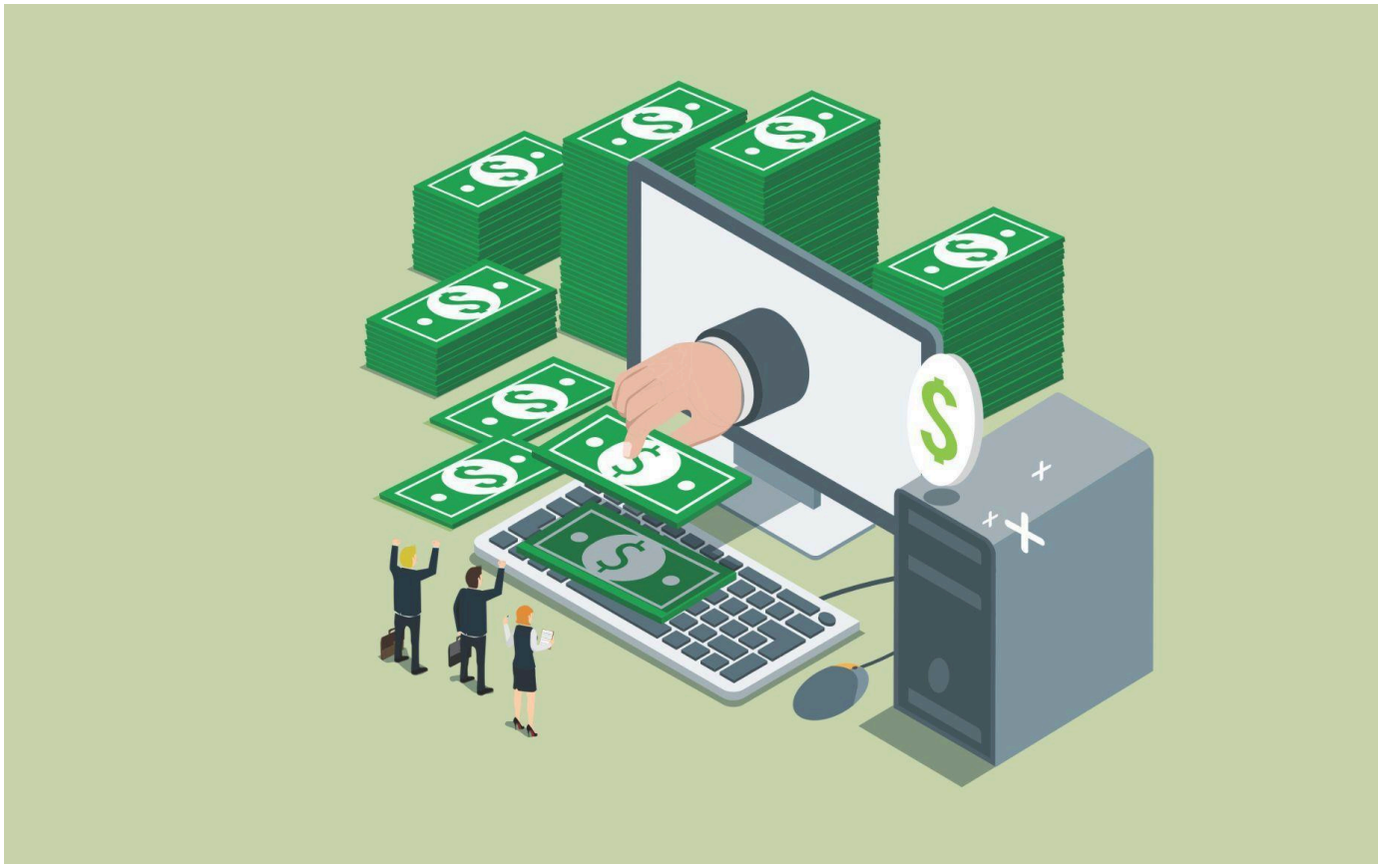
MONTHLY NEWSLETTER

navigate

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

April, 2025

TOP STORY



RBI Governor calls for risk based approach and technology adoption to combat financial crime

By Shivani Shetty

On March 26, the Governor of the Reserve Bank of India (RBI), Mr. Sanjay Malhotra, addressed the Private Sector Collaborative Forum of the Financial Action Task Force (FATF), recognizing India's significant advancements in implementing AML/CFT frameworks. He highlighted the country's efforts in strengthening due diligence procedures, conducting robust risk assessments, monitoring transactions, and reporting suspicious activities to prevent the misuse of the financial system.

In his address, Mr. Malhotra stated that while safeguarding the financial system from money laundering and fraud is crucial, laws and regulations must be designed to specifically target illicit activities without negatively impacting the innocent. He recommended the adoption of a risk-based approach but also acknowledged the challenges of false positives and false negatives. To address these challenges, he emphasized the need for continuous refinement of risk assessment models.

The governor believes that there is a need to improve data quality and utilise emerging technologies to combat financial crime. This will further improve transaction screening and detection of suspicious activities thereby reducing false positives and false negatives. Thus, financial institutions must enable frameworks that allow early detection of suspicious transactions and pre-emptive action.

Financial inclusion remains a key priority, and while India has made remarkable progress, efforts must continue to expand access and ensure that regulatory frameworks do not create barriers. India has made significant strides in digitizing customer onboarding and due diligence (CDD) processes. For example, digital KYC, video KYC and the Central KYC Records Registry (CKYCR), with more than one billion records, have the potential to streamline customer identification. These processes simplify the

onboarding process for customers and can enable regulated entities to perform due diligence more efficiently.

The country has also made significant progress in making cross border payments accessible through fast payment systems and hence there has been growing importance for the FATF Recommendation 16, known as the travel rule. Mr. Malhotra stressed the need for a technology-neutral approach to implementing the travel rule to ensure faster, cheaper and more transparent cross-border payments.

Thus, regulated entities can ensure an inclusive and secure financial sector by continuously refining their AML-CFT framework, integrating technology, and collaborating with law enforcement entities.

Source: The Indian Express

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]

Haryana man arrested for involvement in 43 cases related to trading fraud

The Hyderabad Crime Police arrested a person from Haryana, a mule account supplier involved in over 43 investment and trading fraud cases across India. The case came to light when a 49-year-old civil engineer from Hyderabad received a WhatsApp message promoting high-profit stock investments. Initially, he invested a small sum and successfully withdrew profits using the trading platform. Gaining confidence, he made larger investments, eventually totalling ₹20.01 lakh. When he later attempted to withdraw further returns, he was informed that his money was tied up in IPOs and was asked to deposit an extra ₹15 lakh. Suspecting fraud, he reported the matter to the police.

Source: The Times of India

India and Mauritius sign agreement to combat money laundering

India and Mauritius signed a Memorandum of Understanding (MoU) in the presence of India's Prime Minister Narendra Modi and the Prime Minister of Mauritius Navinchandra Ramgoolam to combat money laundering, fraud, corruption, asset recovery and the financing of illicit activities. This collaboration aims to enhance cooperation and enforcement capabilities between the Enforcement Directorate (ED) and the Financial Crimes Commission (FCC). The agreement will further facilitate joint operations to detect and investigate cross border money laundering operations. Discussions focused on how ED can support FCC by offering technological assistance, sharing digital

forensic tools and best practices to improve data seizure, extraction and analysis. Organisations from both the countries plan to share experiences, organise exchange programs and conduct training for officers.

Source: The Economic Times

4 individuals to be charged for money mule activities in Singapore

Four individuals, aged 17 to 21, have been suspected of involvement in money laundering activities. They allegedly sold their bank accounts or disclosed Singpass credentials to unknown individuals, who then used them to open bank accounts for laundering scam proceeds. The scams included job scams, friend impersonation scams, e-commerce scams, and investment scams. One case involved a 17-year-old receiving $3,000 for sharing his Singpass credentials, which were later used to open an account linked to a phishing scam. The suspects face charges related to money mule activities, including cheating banks into opening accounts, facilitating unauthorized computer access, and disclosing access codes.

Source: The Straits Times

Resorts World casino fined $10.5M for AML compliance failures

Resorts World casino in Las Vegas has been fined $10.5 million for violations related to anti-money laundering (AML) compliance. The Financial Crimes Enforcement Network (FinCEN) found that

the casino failed to implement adequate AML measures, allowing suspicious transactions to go unreported. According to the investigation, the casino did not properly monitor or report large cash transactions, despite clear regulatory requirements. Resorts World has agreed to enhance its AML controls and compliance practices as part of the settlement. This includes improving transaction monitoring systems, staff training, and cooperation with regulatory authorities.

Source: Mint

Rs 2.47 crore bank fraud in Chennai

Law enforcement officials have taken four individuals into custody for their alleged involvement in a Rs 2.47 crore bank fraud. The accused orchestrated the fraud by using forged documents and fraudulent loan applications to siphon off funds from a leading financial institution. The bank officials became suspicious when they detected discrepancies in the loan approvals and repayment records. A formal complaint was lodged, prompting the authorities to take swift action.

Source: Indian Express

STF cracks down on cyber fraud gang running corporate account scams

The Uttar Pradesh Special Task Force (STF) arrested six members of an organized cyber fraud gang, including its mastermind Abdul Malik, for large-scale financial scams involving digital fraud, share market investments, and online gaming. The gang used rented corporate bank accounts to launder money and carried out unauthorized transactions using malicious APK files. The investigation began after a company reported a ₹48 lakh

fraud, where Malik accessed the company's private bank account via malware, conducting 3,200 unauthorized transactions before the bank froze the account. Further investigation revealed that the fraudsters had laundered ₹1.2 crore in January 2025 using a corporate account obtained via Telegram. The STF seized multiple electronic devices, documents, and ₹34,500 in cash, linking them to at least 10 corporate bank accounts and several fraud complaints nationwide. An FIR has been registered against the accused and the investigation is underway.

Source: Hindustan Times

Pune Manager falls victim to ₹3.16 crore matrimony fraud

A 45-year-old manager from Pune was defrauded of ₹3.16 crore by a man posing as a U.S.-based NRI on a matrimonial website. The woman made 350 transactions to 32 different bank accounts, depleting her savings and taking loans. The fraudster claiming business losses and other fabricated emergencies, convinced her to transfer funds with promises of marriage and relocation to the U.S. The woman continued sending money until the man stopped contacting her, at which point she recognised the fraud. Matrimonial frauds use trust as a tool to deceive victims into financial losses and hence it is crucial to remain cautious of financial requests and report suspicious activities.

Source: The Times of India

REGULATORY UPDATE

Financial institutions to directly integrate with I4C to check fraud on accounts

By Neha Joy

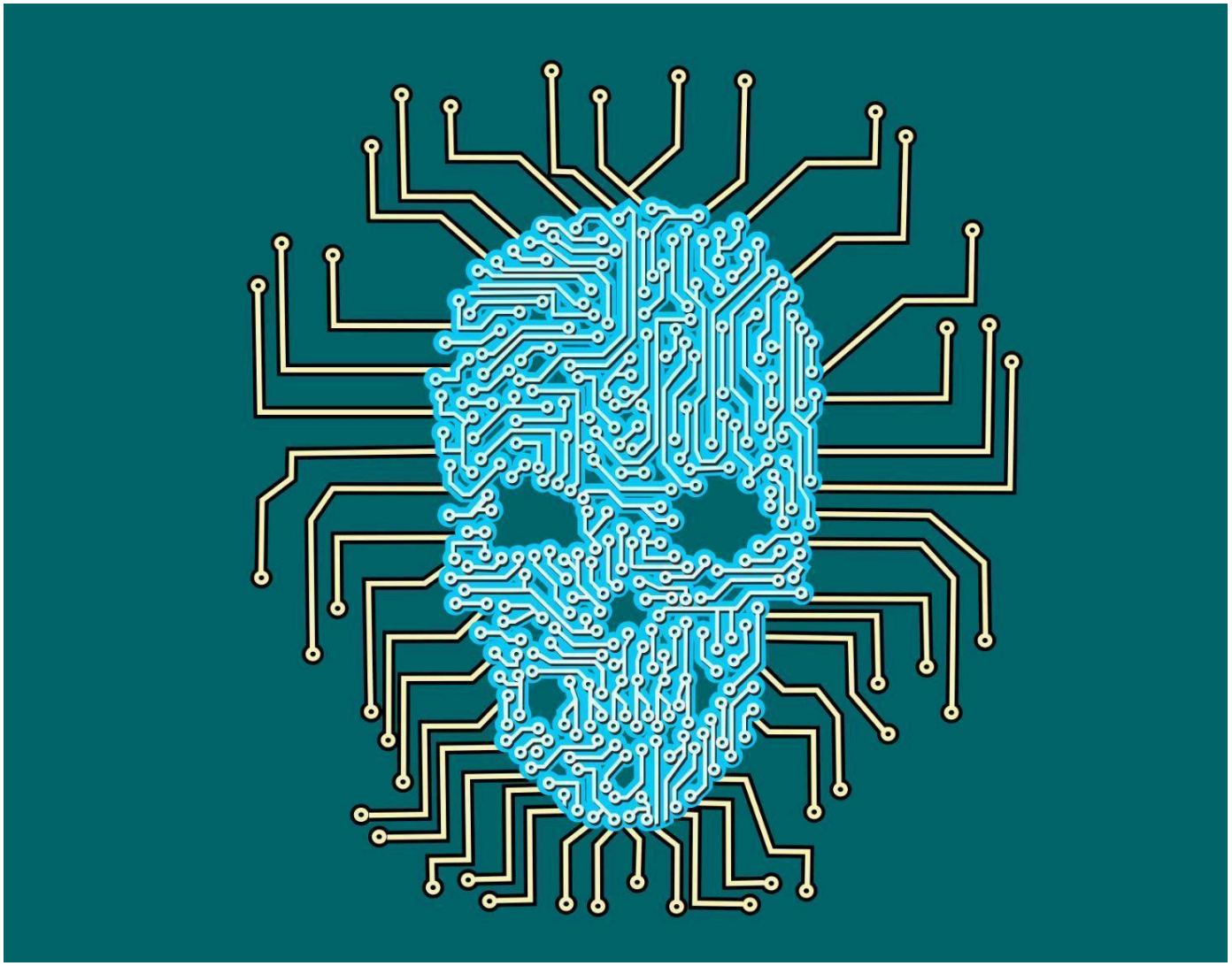
Large banks and payment firms are now directly linking their systems with the Integrated Cyber Crime Coordination Centre (I4C) to take swift action against payment fraud. Previously, when customers filed complaints with I4C, financial institutions received information through manual reports. However, with this new update, alerts will be instantly generated within the financial institutions' system. While several banks have already implemented these integrations, recently, several payment firms like RazorPay and Cashfree have integrated with I4C for real-time fraud prevention, enabling instant alerts and rapid response to fraudulent activities.

The Department of Financial Services has mandated public sector banks to complete API integration with I4C. This integration would ensure that fraud complaints filed through I4C are instantly routed to the relevant financial institution for swift remedial action. Additionally, banks are being encouraged to adopt AI-driven tools such as Mulehunter.AI, developed by the Reserve Bank of India Innovation Hub, to detect and prevent the use of mule accounts, which are often exploited for illicit fund transfers.

Now, with direct integration, fraudulent transactions will trigger automatic alerts within banks' systems, allowing them to take immediate action such as freezing suspicious accounts. Automation decreases the need for manual intervention, leading to cost savings. This not only improves response times but also significantly increases the chances of recovering stolen funds. Apart from preventing fraud, this integration is expected to strengthen trust in digital payments and banking services.

Source: Economic Times

DOMAIN MATTERS



AI-driven financial crime: How technology is empowering criminal networks

By Anna Paulin

Europol has released the EU Serious and Organised Crime Threat Assessment (EUSOCTA) that highlights the use of AI and other new technologies as emerging catalysts for crime. The rapid advancements in AI are making financial crime more dangerous as criminal networks use new tools and tactics to execute and conceal crime.

Cybercriminals exploit AI to automate attacks, enhance social engineering tactics, and evade security defences. AI-driven automation enhances anonymity, allowing criminals to better conceal illicit transactions and obscure the true beneficiaries of illicit financial flows. Criminals use AI's automation capabilities to execute social engineering tactics like large scale phishing campaigns, including phishing-as-a-service operations that distribute emails embedded with malicious macros and files to harvest login credentials.

The advent of generative AI (GenAI) and its accessibility has made it an attractive tool for criminals. With the help of GenAI criminals can now generate messages in various languages, precisely target victims worldwide, and develop advanced malware.

The integration of deepfake technology into financial fraud is further complicating compliance efforts. According to an Economic Times report, fraudsters in Hong Kong used AI-generated deepfakes to deceive the Chief Financial Officer into transferring $25 million. There has been a steady increase in the usage of live deepfake technology and voice cloning by criminal networks, which has led to new forms of fraud, extortion, and identity theft. Further, voice cloning poses a significant risk to institutions that rely on voice authentication as a security measure.

In addition to these fraudulent tactics, the criminal networks employ a new strategic approach known as "Store now, decrypt

later". Fraudsters are collecting and storing encrypted data with the intention of decrypting it once quantum computing becomes advanced enough to break current encryption standards. Since quantum computers could one day crack today's encryption, this poses a serious security risk, and it would lead to leakage of sensitive information from financial institutions, businesses, and individuals. Other emerging technologies like the metaverse, 6G technology, and unmanned systems will further evolve and make the usage of AI for financial crime more anonymous and sophisticated.

To fight against the growing threat of AI-driven financial crime, financial institutions must take a proactive and adaptive approach to prevent fraud. As AI is reshaping digital transactions, institutions must have smarter fraud detection, real-time monitoring, and stronger authentication measures for a safer risk assessment. By improving collaboration and public awareness individuals can recognize and avoid AI-driven financial crime. The fight against financial crime in the AI era is not just about keeping up, it's about staying one step ahead to ensure a safer and more resilient financial system.

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