STORIES THIS MONTH
February, 2025

TOP STORY
Torres Jewellery Scam: A multi-crore fraud exposed

NEWS SNIPS FROM AROUND THE WORLD

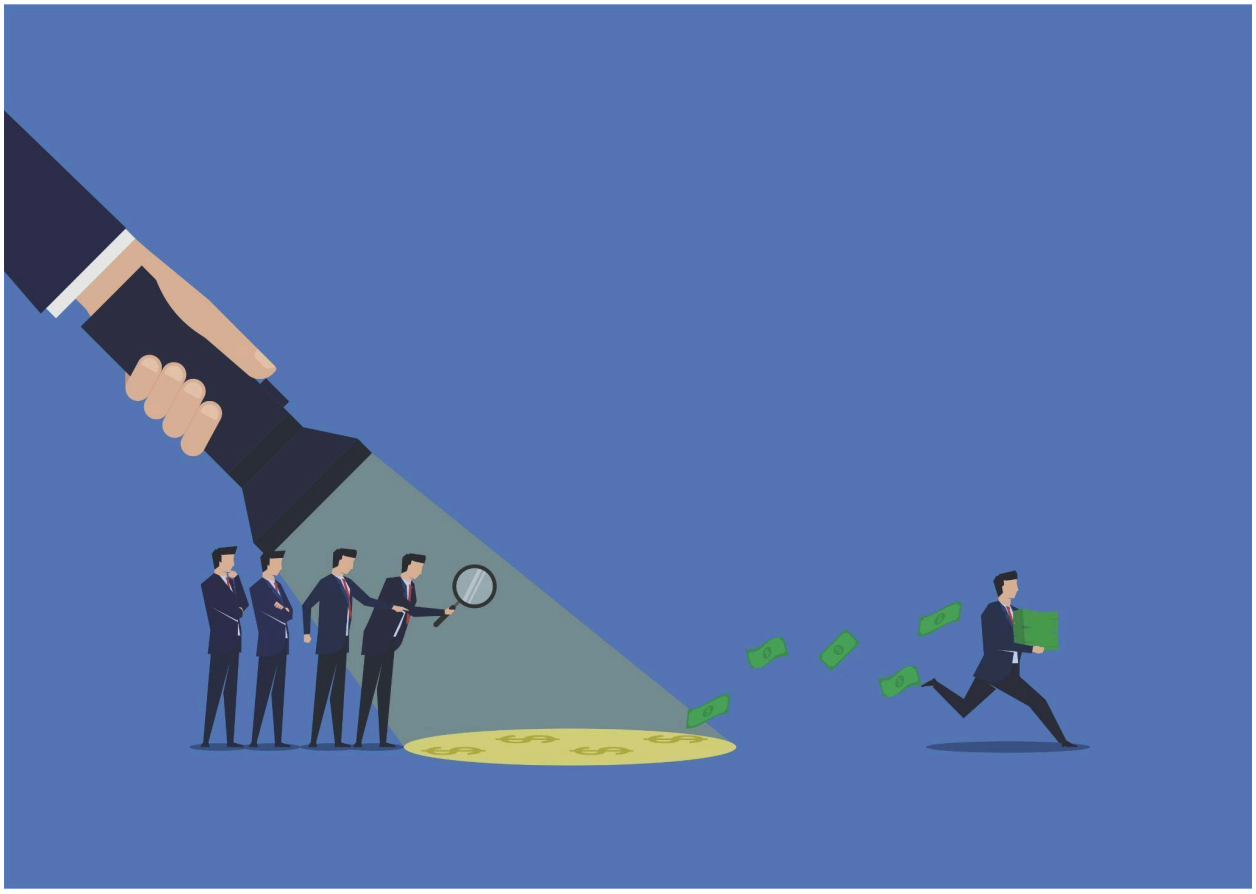
REGULATORY UPDATE
RBI to introduce account look up facility for RTGS and NEFT system

DOMAIN MATTERS
Service-Based Money Laundering and Money Laundering as a Service in TBML

TOP STORY

Torres Jewellery Scam: A multi-crore fraud exposed

by Neha Joy



The Torres Ponzi Scheme is one of the largest financial frauds in recent times. The company is accused of defrauding several investors resulting in losses exceeding ₹1000 Crores.

The scheme was orchestrated by Torres Jewellery, a Mumbai-based company that lured investors with the promise of returns significantly above the market rate. The fraudsters followed a classic Ponzi model, where returns were paid to earlier investors using funds collected from new ones. Ponzi schemes rely on continuous inflow of funds to continue operations making it unsustainable in the long run. Torres Jewellery was eventually exposed when the company failed to sustain payouts, triggering complaints and investigations. Criminals followed a multi-level marketing (MLM) pyramid, which incentivized existing investors to recruit others into the scheme, further amplifying its

scale. This approach not only accelerated fund collection but also helped the perpetrators avoid early detection by authorities.

Large sums of cash were converted into cryptocurrency which was then transferred outside the country. This method allowed fraudsters to bypass legitimate financial channels and evade regulatory investigations. Several reports claim that cryptocurrencies worth approximately ₹200 Crores were funnelled out of India. The outflow bypassed the traditional banking systems for cross-border remittances thus enabling money laundering on a global scale. While Torres Jewellery operated in India, Ukrainian and Turkish nationals were involved in the scheme, prompting Interpol to issue a blue corner notice against them.

This case highlights the need for banks to implement robust AML systems to detect suspicious transactions at an early stage. With the increasing use of cryptocurrency in financial crimes, it is essential for crypto companies to establish strong AML frameworks to mitigate and reduce the risk of financial frauds.

Source: The Economic Times

NEWS SNIPS FROM AROUND THE WORLD

By Anna Paulin

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

FIU-IND and IRDAI sign MoU for enhanced coordination and information sharing

The Financial Intelligence Unit (FIU) - India and the Insurance Regulatory Development Authority of India (IRDAI) have signed a Memorandum of Understanding (MoU) to enhance their efforts in combating money laundering. The agreement aims to facilitate the sharing of intelligence and information between the two entities, strengthening the implementation of the Prevention of Money Laundering Act (PMLA) and other associated rules. The collaboration will focus on areas of mutual interest and enable both organisations to exchange relevant data and insights from their respective database. This partnership highlights the commitment to strengthening coordination and ensuring compliance with anti-money laundering regulations.

Source: PIB

Crypto Exchange BitMEX fined $100 million for violating U.S anti-money laundering laws

The U.S. Department of Justice announced that cryptocurrency exchange BitMEX has been fined $100 million for intentionally disregarding U.S. anti-money laundering laws to increase revenue. BitMEX and its founders, Benjamin Delo, Arthur Hayes, and Samuel Reed, were accused by prosecutors of deliberately violating the Bank Secrecy Act between 2015 and 2020. The alleged violation was due to their failure to implement

Anti-Money Laundering (AML) and Know Your Customer (KYC) programs, highlighting the need for crypto exchanges to comply with regulations.

Source: Reuters

Sri Lanka strengthens AML/CFT framework ahead of APG Mutual Evaluation

Sri Lanka's president Anura Kumara Dissanayake led a high-level discussion on Sri Lanka's preparations for the upcoming Mutual Evaluation by the Asia/Pacific Group on Money Laundering (APG). The meeting, held at the Presidential Secretariat, focused on strengthening the country's anti-money laundering and counter-terrorism financing (AML/CFT) framework. The Financial Intelligence Unit (FIU) emphasized the urgent implementation of cabinet-approved action plans involving 24 key institutions, prioritizing legal reforms, capacity building, and inter-agency cooperation to meet FATF recommendations. The President discussed the formation of dedicated teams to ensure compliance and monitor progress, stressing the need for collaboration and accountability to receive a favourable evaluation and improve financial stability.

Source: PMD Sri Lanka

MHA warns about rise in Pig Butchering Scams

Pig Butchering, a new cyber scam is deceiving people into losing large amounts of money through online platforms. The term "Pig Butchering" refers to fattening up victims with trust and embezzling their money invested in fake cryptocurrency. As per the latest annual report released by the Ministry of Home Affairs (MHA), this 'investment scam' has led to cyber slavery and large-scale money laundering. The Indian Cyber Crime Coordination Centre (I4C) is setting up reporting systems and collaborating with social media platforms to address this threat.

Source: The Economic Times

India and US sign MoU on cybercrime investigations

On 17 January 2025, India and the United States signed an MoU in Washington, D.C. to enhance cooperation in cybercrime investigations. The agreement aims to strengthen cooperation and training in cyber threat intelligence and digital forensics for criminal investigations. The agreement was signed by India's Ambassador to the United States,

Shri Vinay Kwatra, and Ms. Kristie Canegallo, the Acting U.S. Deputy Secretary of Homeland Security (DHS). From India, the Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs (MHA), is responsible for the execution of the MoU. Given the growing complexity of cybercrime and its links to terror financing, extremism, drug trafficking, organized crime, human trafficking, money laundering, and illegal migration, this MoU will improve bilateral security collaboration and further strengthen the global strategic partnership between the countries.

Source: MEA India

Cyber Shield blocks ₹1800 crore worth of online fraud

In nearly three months since the launch of Cyber Shield, an online 'suspect registry,' the Indian government has blocked six lakh fraudulent transactions, saving ₹1,800 crore. Developed by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs, the registry compiles data from the National Cybercrime Reporting Portal (NCRP) and includes 1.4 million cybercriminals linked to financial fraud and cybercrimes. The registry is accessible to states, UTs, and central agencies, aiding in fraud risk management. The Reserve Bank of India has asked all banks to integrate with this system.

Source: The Indian Express

Europol seizes 35.7 million in cash, crypto and assets

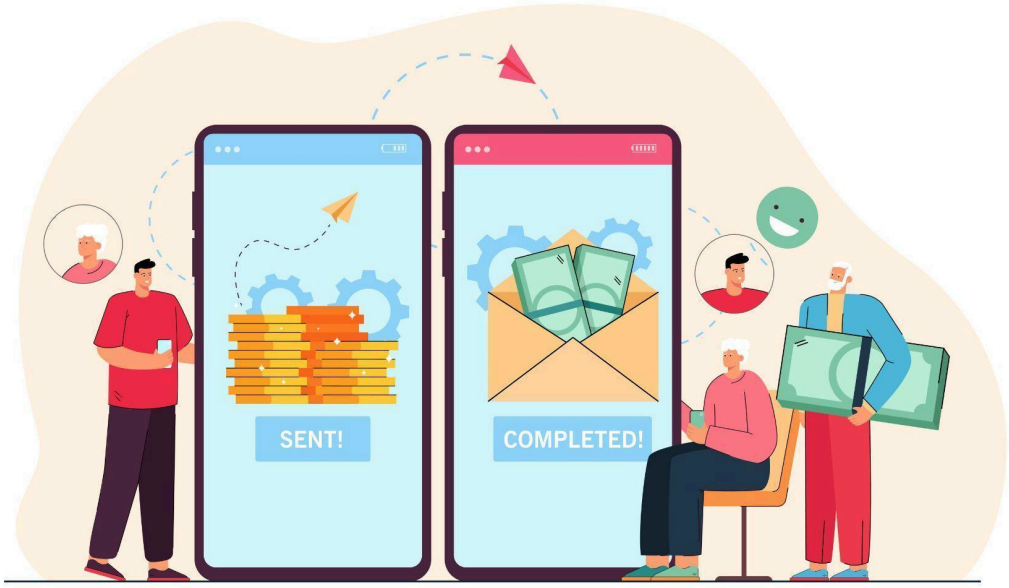
Europol has arrested 23 suspects, primarily Ukrainian nationals who operated a large-scale money laundering and underground banking operation in Spain. The network provided cash courier services to Russian-speaking and Asian criminal groups involved in drug trafficking, tax evasion, and illicit goods smuggling. By taking advantage of EU policies allowing Ukrainian refugees to move cash freely, the network used money mules to transport large sums of money across countries. The criminal network further shifted to the use of cryptocurrencies to evade detection.

Source: Europol

REGULATORY UPDATE

RBI to introduce account look up facility for RTGS and NEFT system

By Shivani Shetty



There are many instances where remitters remitted funds to the wrong beneficiary. To limit the number of incorrect money transfers, the Reserve Bank of India (RBI) has proposed to introduce a beneficiary account name look-up facility for Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) System.

United Payments Interface (UPI) and Immediate Payments Service (IMPS) allow remitters of funds to verify the name of the receiver before making a payment. It has been proposed to put a similar facility for RTGS and NEFT system that would enable a remitter to verify the beneficiary bank account before initiating a transaction.

The National Payments Corporation of India (NPCI) has been directed to develop and implement a system for all banks to offer this facility. Remitters will be able to enter the beneficiary's account number and branch IFSC code, upon which the beneficiary's name will be displayed. The system will retrieve the beneficiary's account name from the bank's Core Banking Solution (CBS) using the account number and IFSC entered by the remitter.

This feature aims to enhance customer confidence by minimizing the risk of incorrect transfers and fraud.

RBI has mandated that all banks, whether direct or sub-members of RTGS and NEFT, must adopt this service by April 1, 2025. The service will be available through internet and mobile banking, as well as for customers making transactions at bank branches. This added layer of security will help reduce the risk of fraud and misdirected payments, particularly in high-value transactions.

Source: The Economic Times

DOMAIN MATTERS

Service-Based Money Laundering and Money Laundering as a Service in TBML

by Amruta Raje

The Financial Action Task Force (FATF) has released several reports addressing different aspects of Trade-Based Money Laundering (TBML), a global threat with widespread consequences. TBML is highly complex and multi-faceted, requiring careful analysis of its many nuances. To effectively combat money laundering, it is necessary to recognise two key concepts: Service-Based Money Laundering (SBML) and Money Laundering as a Service (MLaaS).

Services-Based Money Laundering (SBML) is a distinct form of money Laundering that exploits the trade of services or other intangibles to conceal and legitimize the movement of illicit funds. Assessing the legitimacy of the relationship between the service purchaser and provider becomes challenging, particularly when the underlying service involves consultancy or advisory work. Additionally, the lack of a physical commodity that generates import or export data further complicates the detection and analysis of SBML activities.

Some businesses are particularly vulnerable to Service-Based Money Laundering, including online gambling service providers, software providers, financial services, consultancy, advisory services providers, as well as transactions involving trademarks and other intangible assets such as intellectual property rights. Since these services are legitimate on the surface, identifying laundering activities requires thorough due diligence and vigilance.

Adding another layer of complexity, criminals now offer Money Laundering as a Service (MLaaS), a business model where third parties provide money laundering services to others, typically for a fee. MLaaS providers use a variety of techniques to assist their clients, such as structuring transactions, moving funds through multiple jurisdictions and exploiting the anonymity of virtual assets.

Unlike traditional money laundering methods that often involve physical goods or commodities, specialized MLaaS for SBML primarily operate by exploiting intangible services, which adds an additional layer of difficulty for authorities in detecting suspicious activities. These providers offer tailored services, ranging from creating fake business contracts and inflating service costs to facilitating complex cross-border financial transfers that disguise the illicit nature of the funds. Some of the most exploited services in MLaaS include consultancy, advisory services, software development, virtual asset management, and intellectual property rights transactions. These service-based channels allow MLaaS providers to move illicit funds across borders without triggering traditional financial reporting mechanisms like customs declarations or import/export documentation.

The anonymity and complexity of digital financial platforms used to facilitate MLaaS, combined with the evolving sophistication of SBML techniques, means that specialized money laundering services are becoming a critical tool for criminals. Specialized MLaaS providers are increasingly exploiting service-based industries to facilitate the laundering of illicit funds.

To counter the misuse of service-based industries for money laundering, authorities are increasingly focusing on scrutinizing financial services, digital transactions, and intangible assets. Through the implementation of advanced monitoring technologies, financial institutions can detect suspicious transactions and identify patterns of SBML and MLaaS activities.

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