EUR 300 million credit card fraud| Vietnam introduces new AML guidelines| How Professional Money Launderers exploit the global trade system and more

December , 2025

TOP STORY

EUR 300 million global credit card fraud

By Neha Treesa Joy

A major international crackdown by Eurojust (European Union Agency for Criminal Justice Cooperation) resulted in the arrest of 18 suspects linked to a global credit card fraud scheme, organised through three separate networks, that impacted millions of credit-card users worldwide and stole at least €300 million.

The scheme exploited stolen credit card data to create nearly 19 million fake online subscription accounts across a range of services, including dating, pornography, and streaming platforms. The victims were unknowingly enrolled on recurring payments. Over 4.3 million cardholders across 193 countries are estimated to have been affected.

The suspects were involved in stealing sensitive card information, setting up fake accounts, authorising and concealing payments, and money laundering. Monthly payments were deliberately kept below €50 to avoid creation of suspicion. Transaction descriptions were vague or obscure, and many of the fraudulent websites were intentionally made unsearchable on the internet and accessible only through direct links or URLs. This design helped conceal the scheme and prevented victims from discovering misuse of their credit cards.

Further, the infrastructure of four payment providers was exploited to launder the illegal proceeds of the fraud. Employees of the payment services colluded with the fraud networks to use the financial infrastructure. The suspects used a series of shell companies to conceal their activities and distribute the fraudulent transactions. These companies were obtained through ‘crime as a service’ providers, where they assist the criminals in their illicit activities against a fee.

More than 60 raids were conducted across multiple countries, including Germany, Luxembourg, Canada, Singapore, the U.S., and several EU member states. As part of the operation, millions of euros in assets were seized, and critical digital evidence was collected, including documents, phones, laptops and transaction records. The

investigations are being further supported through mutual legal assistance between countries, making use of cross-border cooperation frameworks.

Source: EUROJUST

NEWS SNIPS FROM AROUND THE WORLD

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

₹58 crore digital arrest scam uncovers transnational money-laundering network

Investigations into a Rs 58 crore digital arrest scam have found that a major portion, Rs 15.25 crore, was funnelled into a Gujarat firm's bank account. The scam began when a couple were duped by cybercriminals posing as officials from central agencies, who used fake video calls and staged courtrooms to coerce them into transferring their life savings under the guise of an "investigation." The Maharashtra Cyber Police arrested the firm owner and four others, identifying the account as a medium for laundering the proceeds of the fraud. The investigation revealed that funds moved through 27 mule accounts across Maharashtra, Gujarat, and Rajasthan before being transferred abroad, with links to China, Dubai, and Cambodia, indicating a transnational cybercrime network.

Source: The Times of India

China's 'Cryptoqueen' jailed in UK over $6 billion crypto scam

Qian Zhimin, widely referred to as 'China's Cryptoqueen,' masterminded a Ponzi-style investment drawing in more than 128,000 victims and generating an estimated US $6.4 billion in illegal profits. Police said she ran a pyramid scheme that lured more than 128,000 people to invest in her business, including many who invested their life savings and pensions. A significant portion of investor funds was converted into cryptocurrency. The UK police seized digital wallets containing over 61,000 BTC, marking the largest cryptocurrency seizure in British history. Qian was eventually arrested in the United Kingdom and prosecuted under money-laundering legislation, not for the original Ponzi scheme in China, but for holding and transferring criminal property in the form of Bitcoin and other proceeds.

Source: CNN

Ireland's Central Bank fines Coinbase Europe 21.5 million euros over monitoring failures

Ireland's central bank fined Coinbase Europe for shortcomings in its anti-money-laundering and counter-terrorist-financing transaction monitoring. Due to coding errors in Coinbase Europe's monitoring system, over 30 million transactions worth more than €176 billion were not properly screened between 2021 and 2022. Coinbase took nearly three years to finish reviewing the affected transactions, ultimately reporting 2,708 suspicious cases involving potential crimes such as money laundering, fraud, drug trafficking and child exploitation. Three coding mistakes caused five of 21 monitoring scenarios to fail but Coinbase fixed them within weeks of discovery and has since enhanced its testing and monitoring.

Source: Reuters

ED freezes 110 mule accounts in drug-linked money-laundering case

India's Enforcement Directorate (ED) froze 110 mule bank accounts, seized ₹70 lakh in cash, and uncovered the use of Dubai-based cryptocurrency wallets during raids linked to a money-laundering investigation. The money laundering investigation was tied to a drug trafficking case involving cocaine worth about ₹900 crore. The searches undertaken across Delhi-NCR and Jaipur revealed an online betting and gambling network being operated through mobile apps for concealing the drug proceeds. The operation resulted in the freezing of mule accounts, including 73 linked to UPI IDs and digital wallets that were actively being used for handling transactions related to the betting operations.

Source: The Hindu

Five indicted on €188 Million VAT fraud and money laundering

European Public Prosecutor's Office (EPPO), through its Hamburg office, formally indicted five individuals, three Danish citizens and two Turkish nationals residing in Germany, on charges related to a broad VAT fraud scheme and money laundering. The fraudsters are accused of participating in a criminal organisation focused on the sale of electronic goods, in many cases, having existed only on paper without legitimate business activity. Invoices, fake deliveries, bogus invoices and fictitious customers helped simulate legitimate trade flows, while VAT owed on goods was never properly paid. According to the investigation, the group set up shell companies across several EU Member States to carry out the fraud. In addition, the defendants are accused of founding a blockchain company to launder the profits by purchasing cryptocurrency.

Source: EPPO

REGULATORY UPDATE

Vietnam introduces new AML/CFT guidelines

By Neha Treesa Joy

Vietnam has recently strengthened its anti-money laundering (AML) and counter financing of terrorism (CFT) framework by introducing a risk management framework and reporting requirements.

As of November 1, 2025, any domestic money transfer equal to or exceeding VND 500 million must be reported to the State Bank of Vietnam (SBV)'s Anti-Money Laundering Department. Cross-border transfers of US$1,000 or more are also now subject to reporting requirements. The reporting obligations cover both individuals and

organisations. Reports must include details such as the identities of the sender and receiver, the purpose of the transfer, the source of the funds, and relevant transaction documentation.

According to the circular, all reports should be submitted exclusively through digital channels, and institutions should file them electronically using the prescribed data format. The full digitalisation of reporting processes is expected to improve transparency and reduce risks associated with manual processing.

The country has taken steps to align its domestic AML compliance more closely with international standards recommended by bodies such as the Financial Action Task Force (FATF). Financial institutions shall adopt a risk-based approach and classify customers by money laundering risk levels (low, medium and high) based on factors such as customer type, products and services, geographic areas and other factors determined and classified by the reporting entity as suitable to the reality and specified in their risk management process.

Entities are expected to maintain adequate internal AML policies that match their risk level, periodically review and update them, and ensure all employees or staff undergo AML training within a defined timeframe to improve the quality of internal controls. In addition, strengthening transaction monitoring is expected to enable authorities to detect unusual money flows earlier and reduce the possibility of suspicious funds circulating unnoticed within the economy. These steps can help organisations prevent money laundering and stay compliant with regulations.

Source: Viet Nam News

DOMAIN MATTERS

How Professional Money Launderers (PMLs) exploit the global trade system

By Shivani S.

Professional Money Launderers (PMLs) provide ML services in exchange for a commission, fee or other type of profit. These individuals use specialised knowledge and expertise to exploit legal loopholes and help criminals legitimise the proceeds of crime. The ability of PMLs to combine legal and illegal activities makes them highly effective service providers for organised crime groups.

A Professional Money Laundering Network (PMLN) is a group of associates or contacts working together to carry out money-laundering schemes or subcontract specific services. These networks often operate across borders and may involve two or more PML operators working in coordination. PMLNs facilitate sophisticated laundering processes through the opening of foreign bank accounts and creating or purchasing companies abroad.

PMLNs use a wide variety of ML tools and techniques. Some widely used mechanisms include Trade Based Money Laundering (TBML), account settlement mechanisms and underground banking.

TBML involves disguising proceeds of crime by integrating them into legitimate trade transactions. It is the process of moving or concealing value through trade to hide the illicit origin of funds. Common TBML methods used by PMLNs include

- Purchase of high-value goods: High-value goods are bought with illicit funds, followed by shipping and reselling these goods abroad
- Phantom shipments: The transfer of funds that are claimed to be linked to trade or the purchase of goods, even though the goods are never actually shipped or delivered.
- Over or under-invoicing: Faking the quantity or value of goods listed in shipping documents so they appear higher or lower than the actual payment, enabling criminals to move or receive illicit funds under the guise of legitimate trade.
- Using illicit proceeds to buy goods: Illicit proceeds are used to buy goods that are then sold through legitimate businesses, where the legitimate buyers make payments that ultimately go to the drug traffickers or distributors.
- Money (Peso) brokers: Money (Peso) brokers are third parties who purchase drug proceeds in the location where illicit proceeds are generated by drug cartels e.g. Colombia, Mexico at a discounted rate. Money brokers often employ individuals who collect narcotics proceeds and then move or distribute those funds, as directed by the

drug trafficking organisation or the money brokers who serve as professional money laundering organisations.

PMLs may also create and use false documents, structure multiple financial transactions and set up shell companies to support fake trade activities. Through these TBML methods, they can break the link between the original crime and the laundering process, making it harder to associate the criminal actors with the money laundering activity.

Thus, Professional Money Launderers and their networks play a critical role in enabling modern criminal activities. Understanding how these networks function can help improve efforts to monitor, detect and prevent money laundering operations.

Source: FATF

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.