Major money laundering scheme dismantled in Spain | Bank of Thailand tightens AML regulations | Common threats linked to stablecoins and more

April, 2026

From the dismantling of a money laundering scheme exploiting vulnerable women to stricter AML regulations on cash and crypto, financial crime management is constantly changing across borders. This edition covers global cases, risks and regulatory expectations shaping the fight against money laundering.

TOP STORY

Major money laundering scheme dismantled in Spain

By Neha Treesa Joy

An international law enforcement operation led by Spanish authorities, European Union Agency for Law Enforcement Cooperation (Europol) and International Criminal Police Organization (Interpol) has dismantled a major money laundering network that exploited vulnerable Ukrainian women.

The operation resulted in the arrest of 12 suspects and exposed a complex cross-border financial crime scheme that specifically targeted Ukrainian women who had fled the ongoing conflict in Ukraine. The victims were in extremely vulnerable situations in areas heavily impacted by the war in Ukraine and were completely under the control of the suspects.

The network followed a structured modus operandi using money mules and stolen identities. Initially, the criminal network opened bank accounts using the stolen data of Spanish citizens. As the operation evolved, the group started recruiting vulnerable Ukrainian women as money mules and coerced them into opening bank accounts. Women were also brought to Spain and made to open bank accounts, which were then controlled by the criminals. These accounts were further used to obtain credit cards, which were linked to online gambling platforms. The network created gambling accounts, some under stolen identities and others in the names of the recruited women. Through automated systems, high-volume betting activities were conducted, disguising the origin of illicit funds as legitimate winnings.

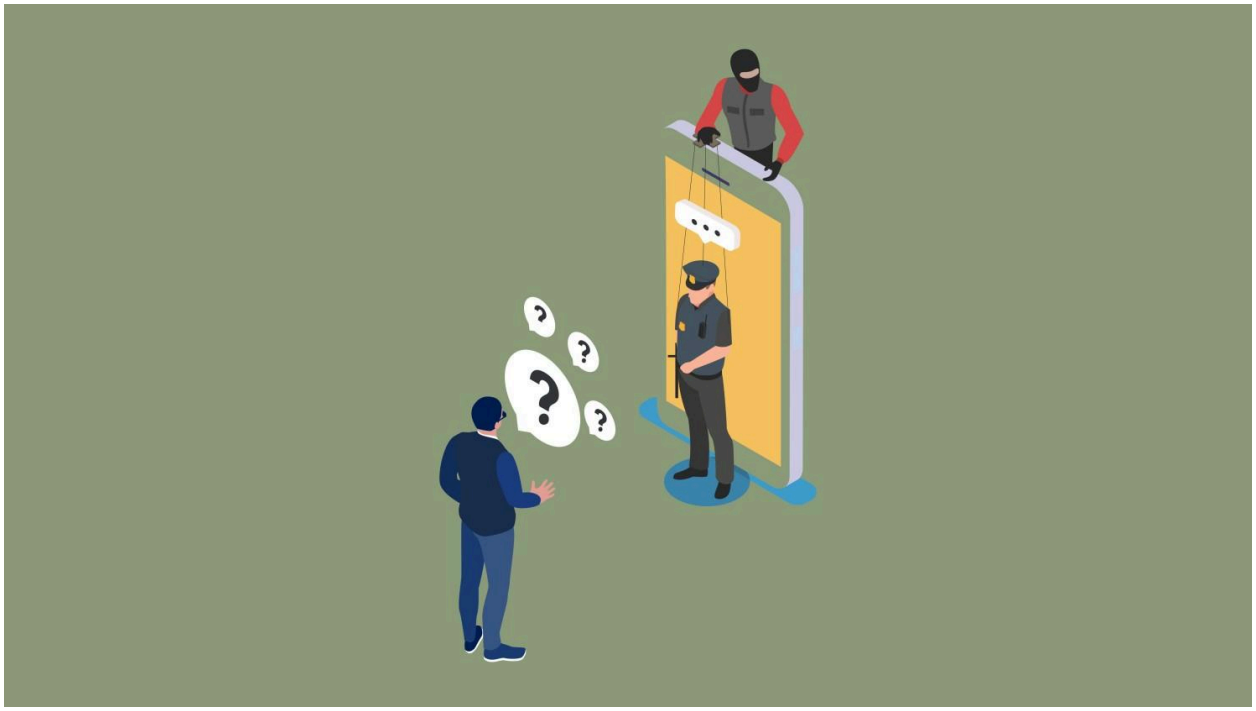
The misuse of bank accounts, credit cards, and identities allowed the network to move funds while avoiding detection. The illicit proceeds were withdrawn, transferred across a wide network of accounts, and in some cases reinvested into high-value assets such as

luxury real estate. The operation emphasises the need for stronger due diligence, better monitoring of transactions, and improved safeguards to prevent human exploitation to facilitate cross-border money laundering.

Source: EUROPOL

NEWS SNIPS FROM AROUND THE WORLD

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



FinCEN Expands Border Reporting Order to Target Cartel-Linked Cash Flows

To prevent drug cartel financing and associated criminal activity, the Financial Crimes Enforcement Network (FinCEN) has issued an expanded Geographic Targeting Order (GTO) requiring specific money services companies along the southwest U.S. border to report smaller cash transactions. Businesses in specific countries and ZIP codes in Arizona, California, New Mexico, and Texas are required by the order to file Currency Transaction Reports for cash transactions totalling $1,000 to $10,000. The action is meant to help prevent people and organisations connected to drug trafficking

organisations from utilising the U.S. banking system, improve law enforcement's access to financial intelligence, and produce investigative leads.

Source: FinCEN

South Korea imposes a penalty on Bithumb for AML violations

South Korean financial authorities have imposed a six-month partial business suspension and a 36.8 billion KRW fine on Bithumb, the country's second-largest cryptocurrency exchange, for failing to meet anti-money laundering (AML) and customer verification requirements. Bithumb was found to have processed 45,772 transactions with 18 unregistered overseas exchanges, despite repeated warnings to stop such activities. Violations were linked to failures in completing verification procedures, allowing transactions without proper verification and a lack of retention of required customer documentation.

Source: The Chosun Daily

Canadian authorities revoke crypto firms' registrations

Canadian anti-money laundering authorities have recently intensified their focus on cryptocurrency businesses, revoking the registrations of nearly three dozen firms. These Toronto based Crypto businesses were found to be operating without the required FINTRAC registration to deal in virtual currencies. Many of these unregistered businesses specialised in the conversion of cryptocurrency into physical cash. This led to Canada's Financial Transactions and Reports Analysis Centre (FINTRAC) removing 23 crypto companies from its registry of permitted money services businesses.

Source: International Consortium of Investigative Journalists

Canaccord Genuity LLC fined $ 80 million for BSA violations

Canaccord Genuity LLC (Canaccord) was assessed by the Financial Crime Enforcement Network (FinCEN) and levied its biggest ever fine worth $80 million for wilful violations of the Bank Secrecy Act (BSA). It has been estimated that 160 suspicious activity reports (SARs) on the trading of over-the-counter securities were not filed by Canaccord. The institution lacked measures such as risk-based Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and onboarded high-risk clients with alleged connections to illegal actors. It also did not set up and implement internal controls to monitor suspicious transactions. These compliance failings resulted in significant economic harm to innocent investors.

Source: FinCEN

Ten arrested in casino money laundering scheme

Taiwanese authorities uncovered a large money laundering network linked to casinos in Macau. The operation involved an online gambling network and two individuals who funneled illicit proceeds through money mules' credit card accounts, making prepayments to increase spending limits. The recruited money mules were sent to Macau, where they used the credit cards at local casinos, purchased chips, simulated gambling activity and converted the chips back into the local currency. The investigation has been completed, and 10 people have been charged under the Money Laundering Control Act and related legislation.

Source: Taipei Times

Rs. 15.4 crore digital arrest scam

An 81-year-old businessman in Belagavi was defrauded of Rs 15.4 crore through a sophisticated digital arrest scam. The fraud began with a phone call from an individual posing as a CBI officer, falsely claiming that the victim's bank account was linked to a money-laundering case. Fraudsters convinced the victim to share sensitive financial details and transfer money in multiple phases. The victim was persuaded to liquidate long-held stock investments under the pretext of "verification" and to transfer funds in multiple transactions, ranging from Rs 1 crore to Rs 2.5 crore, over a month. The fraudsters used layered bank transfers to obscure the money trail. Police have frozen several bank accounts linked to the case.

Source: The Times of India

REGULATORY UPDATE
Bank Of Thailand Tightens its AML Regulations

By Adhila Thirumalai

The Bank of Thailand (BOT) has tightened controls on cash-related transactions to combat the use of financial institutions as channels for illicit funds. Since cash remains one of the main means of concealing the origins of illicit funds, the new framework aims to monitor cash withdrawals and transactions involving cashier's cheques that lead to cash withdrawals.

BOT strengthens its customer due diligence (CDD), enhanced due diligence (EDD) and risk management norms through the following guidelines:

- Complete customer verification before processing any cash transaction, applicable to both physical branches and digital channels. ID card/passport, contact details and a signature are required for physical branch verification and PIN, OTP, and biometrics for digital channels.
- Request customers to clearly state the purpose of a cash transaction and monitor its consistency with the customer's profile.
- Refuse transactions if the customer cannot justify the purpose or provide the required documents.
- Any cash transaction of 5 million baht or more within a single day is to be treated as high risk and necessitate immediate EDD.
- Maintain transaction records and ensure their availability for investigations and regulatory review.

The Bank of Thailand will implement this new framework from 1st April 2026 to strengthen and prevent the exploitation of legitimate institutions. The BOT intimates the potential to expand supervision later to other types of cash transactions, including cash deposits and banknote exchange services, if the risk rises further. The continued reporting of suspicious transactions to the Anti-Money Laundering Office in accordance with the relevant laws and maintaining systems to monitor, detect, and review customers' cash transaction behaviour on an ongoing basis can enhance the transparency of the financial system.

Source: The Nation

DOMAIN MATTERS

Stablecoins and unhosted wallets: Threats and Best Practices for Mitigation

By Shivani S.

Stablecoins like Tether (USDT) and USDC are cryptocurrencies designed to maintain a stable value by pegging themselves to reserve assets, usually the U.S. dollar, offering a low-volatility alternative for crypto trading, payments, and remittances. Stablecoins have rapidly become common in the virtual asset ecosystem, offering speed, low transaction costs, and price stability. However, these same features have made them highly attractive for money laundering (ML) and other illicit financial activities. Today, stablecoins account for a significant majority of illicit crypto transaction volumes, surpassing more volatile assets like Bitcoin and Ether.

Common Threats

The following are some common threats linked to stablecoins

- Money Laundering: Criminal actors increasingly use stablecoins to move illicit proceeds due to their liquidity, interoperability, and ease of cross-border transfer. Stablecoins are commonly used to collect proceeds from crimes such as investment fraud, impersonation fraud and romance scams. Criminals often request payments in stablecoins and exchange stablecoins for fiat currency, completing the money laundering cycle.
- Drug Trafficking: Drug trafficking organisations use stablecoins for procurement, where transferred stablecoins are converted into local currency or reinvested into further drug production. Traffickers also exploit online gambling platforms and merchant refund loops to legitimize funds, where goods are purchased using stolen identities and returned for refunds in stablecoins to third-party wallets.
- Professional Money Launderers: Perpetrators use techniques such as smurfing (splitting transactions into smaller amounts) and cross-chain transfers to obscure the origin and destination of funds. They frequently rely on unregulated or non-compliant Virtual Asset Service Providers (VASPs), decentralized exchanges, mixers, and peer-to-peer platforms.

Best Practices for Mitigation

VASPs can adopt the following controls to mitigate these risks:

- Due Diligence: Apply customer verification processes, counterparty due diligence and enhanced due diligence, particularly for high-risk users and transactions involving unhosted wallets.

- Risk-based controls: Conduct a risk assessment to identify risks related to stablecoins and unhosted wallets. Based on this assessment, implement appropriate controls such as limiting or flagging transactions involving unregistered or non-compliant VASPs and high-risk jurisdictions.
- Transaction Monitoring: Implement a transaction monitoring system to detect suspicious patterns such as rapid transfers, chain-hopping, and interactions with high-risk addresses or sanctioned addresses.
- Travel Rule: Ensure travel rule compliance, which involves the sharing of sender and recipient information for virtual asset transfers.

While stablecoins and unhosted wallets offer significant benefits, they also present several risks. Their speed, accessibility and anonymous nature make them attractive to illicit actors, and hence it is essential for VASPs to adopt strong risk mitigation measures.

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.