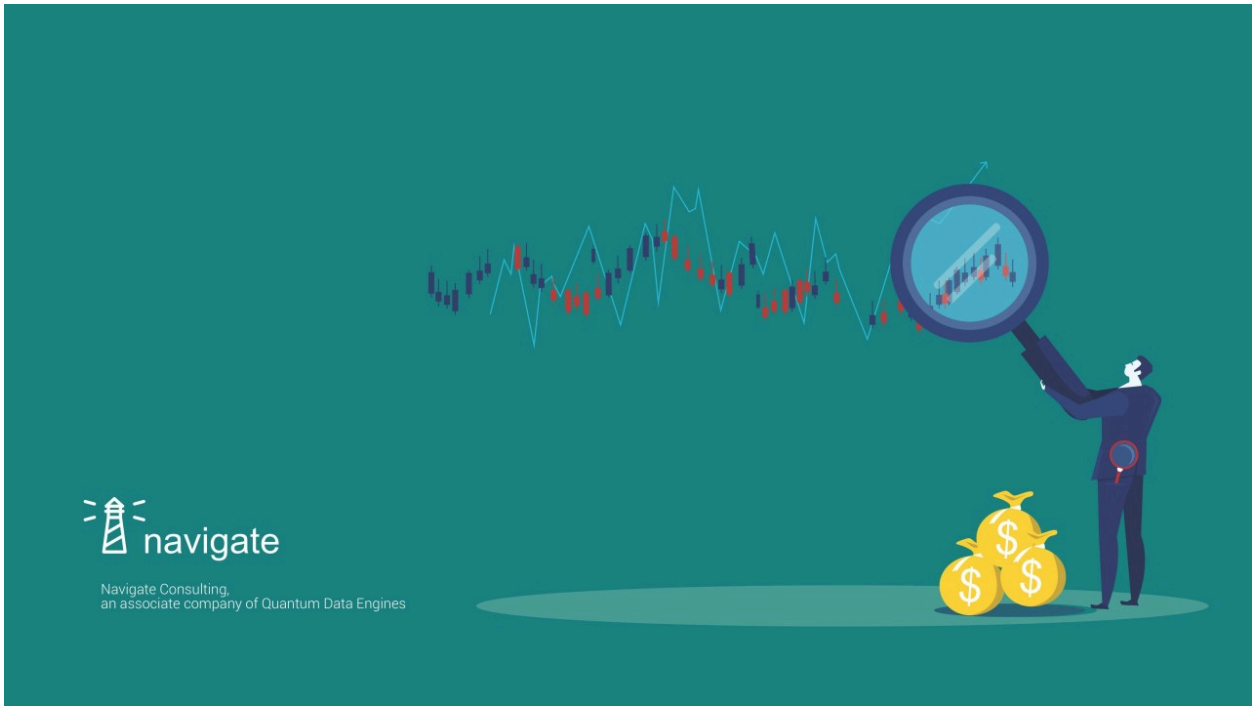


Money laundering through unauthorised forex trading| FINMA supervision in 2025| FBI Internet Crime Report and more

June, 2026

As financial crime threats grow in complexity, regulators and law enforcement agencies are increasing their focus on prevention, detection, and enforcement. This issue highlights money laundering risks linked to unauthorised forex trading, FINMA's latest supervisory findings, key takeaways from the FBI Internet Crime Report and other developments in the AML and fraud domain.

₹500,000 Million Money Laundering and Cyber Fraud Case: Lessons for Financial Institutions

For more details write to: connect@navigate-change.com

By Shivani Shetty

An international online forex broker, operating globally since 2011, was identified as a key beneficiary in multiple linked suspicious transactions. The Egmont Group, in its Annual Report 2024-25, covered how the Financial Intelligence Unit-India (FIU-IND) disrupted a money laundering and cyber fraud network that operated through unauthorised forex trading. Over its five years of unauthorized operation, the platform generated over ₹500,000 million in proceeds of crime. Ultimately, it was the combined effort of FIU-IND, the Enforcement Directorate (ED), international partners and financial institutions that led to the criminal prosecution and detection of the fraud operation.

Modus Operandi

To build publicity and draw investors, the platform was promoted on social media sites, through influencers and advertisements. Investors were asked to transfer funds directly to bank accounts of shell companies posing as e-commerce entities, enabling access to payment gateways. Dummy directors of these shell companies were trained by ex-bankers who were involved in the illegal activity to respond to queries from banks. The platform incentivised traders through gifts and cars. The firm operated as a B-book broker, intermediating trades internally and often trading against its own users, profiting from their losses. The profit made through illegal trading was siphoned offshore through shell companies using fake imports of services.

Money Laundering Typologies

The network employed various laundering and layering techniques to hide the illicit activity including.

- Mule Accounts: Shell companies acted as mule accounts to collect investor's funds, concealing ownership and enabling payment gateway access. These payment aggregators were further misused to bypass KYC norms.
- Regulated Alternate Investment Funds (AIFs): Some laundered proceeds were also invested in alternative investment funds as an attempt to legitimize the money.
- Trade-based money laundering: Funds were layered through shell companies using fabricated invoices to transfer money overseas under the guise of paying for imported services.
- Foreign Direct Investment: Illicit proceeds were reintegrated into the Indian economy as foreign direct investment (FDI) into the firm, successfully hiding their illegal origin.

Best Practices

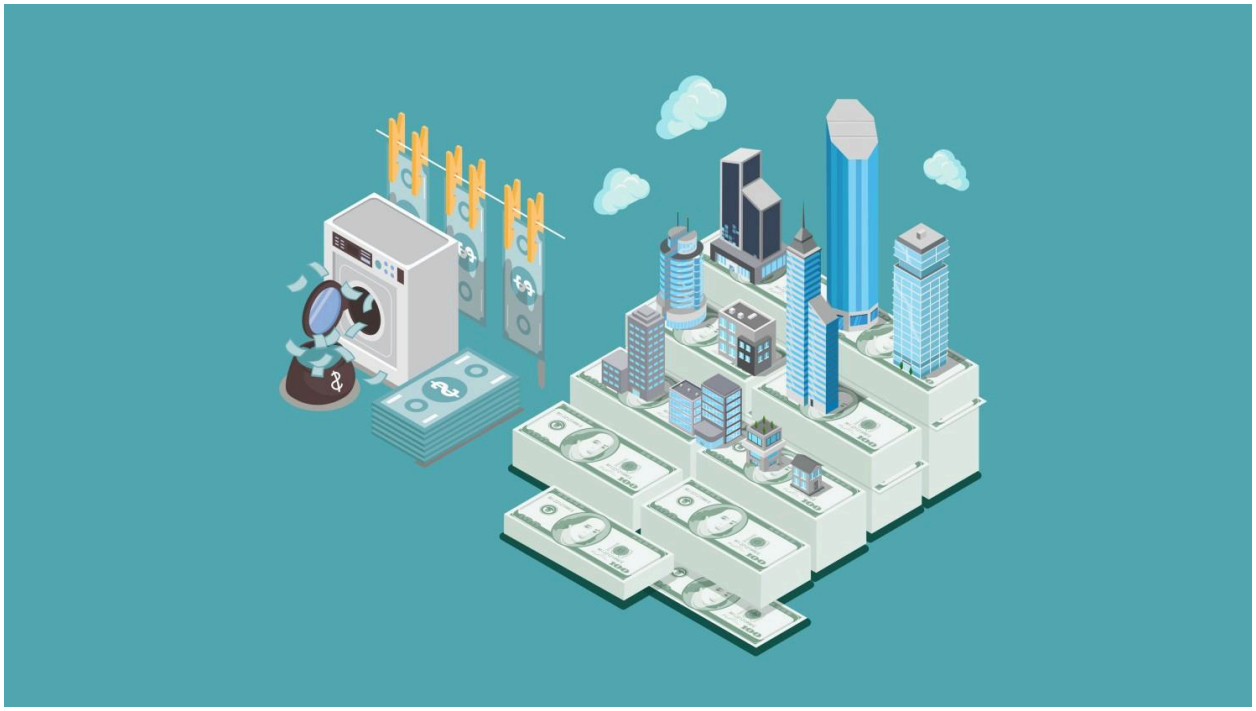
The investigation process involved analysis of several bank statements as well as identification of dummy and mule account holders through KYC forms and Suspicious Transaction Reports (STRs). The investigation also demonstrated the value of utilising open-source intelligence (OSINT) and registry databases to identify foreign assets and properties linked to the accused individuals.

It is crucial that illicit activities such as unauthorised forex trading are promptly reported to support timely investigation and reduce financial losses. Effective filing and analysis of Suspicious Transaction Reports (STRs) can significantly aid in identifying mules, shell companies and other facilitators of financial crime. Since mule accounts were extensively used to collect, layer, and divert illicit funds, financial institutions can implement monitoring scenarios capable of detecting mule activity, supported by advanced link-analysis technologies. The case exhibits the role of strong domestic and international intelligence-sharing frameworks, the adoption of AI/ML driven monitoring systems and

the integration of cybercrime and financial crime investigations in financial crime detection and prevention efforts.

NEWS SNIPS FROM AROUND THE WORLD

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



U.S. Treasury Sanctions Sinaloa Cartel Networks Over Fentanyl and Money Laundering

The U.S. Department of the Treasury has announced sanctions against more than a dozen individuals and entities linked to the Sinaloa Cartel's fentanyl trafficking and money laundering operations. The action, taken by the Office of Foreign Assets Control (OFAC), targets two major networks involved in drug trafficking, bulk cash movement, and

cryptocurrency-based laundering activities. The network used digital assets to move proceeds from fentanyl and other narcotics sales while attempting to conceal the origin of funds. The sanctions also targeted a second trafficking and laundering network accused of operating drug distribution activities across multiple U.S. states and laundering proceeds for the cartel.

Source: U.S. Department Of the Treasury

30 arrested in a joint operation targeting romance scams, fraud and money laundering

More than 30 people were arrested in a joint UK–Nigeria crackdown targeting organised cybercrime networks involved in romance scams, online fraud, and money laundering. The suspects allegedly operated sophisticated scams in which fraudsters built emotional relationships with victims online over long periods before persuading them to send money. Investigators found that the criminal networks also used stolen banking information, fake online identities, and money-laundering channels to move and conceal the proceeds of the fraud. During raids across Europe and Africa, police seized cash, luxury watches, electronic devices, and other evidence linked to the scam networks.

Source: Times Of India

I4C Signs MoU with Reserve Bank Innovation Hub

The Indian Cyber Crime Coordination Centre (I4C) has signed a Memorandum of Understanding with the Reserve Bank Innovation Hub to enhance cooperation in combating cyber-enabled financial fraud and detecting mule accounts within the banking and digital payments space. The agreement focuses on collaboration in fraud-risk intelligence sharing, analytical assistance and operational coordination to strengthen proactive fraud detection and prevention systems.

Source: Akashvani News

2 Chinese citizens indicted for conspiring to launder money linked to drug cartels

Ruhuan Zhen and Hongce Wu allegedly helped conceal the origins of illicit funds for multiple transnational criminal organizations, including the Sinaloa Cartel and the Cartel de Jalisco Nueva Generación (CJNG). Between November 2016 and April 2025, Zhen, Wu, and their co-conspirators are accused of laundering large amounts of cash generated by drug trafficking operations. They employed a range of money-laundering techniques, including mirror transfers, use of overseas bank accounts, encrypted messaging platforms, trade-based laundering and methods designed to evade serial-number verification systems. The network operated across the United States, Mexico, Latin America, and China, processing proceeds from the import and sale of illegal drugs such as cocaine and fentanyl.

Source: South China Morning Post

₹70 crore money laundering case

A man from Mumbai was arrested by the Enforcement Directorate (ED) in connection with a ₹70 crore money laundering case linked to alleged financial fraud and illegal transactions. The proceeds of crime from extortion and cheating were layered and laundered through multiple bank accounts, cooperative credit societies, movable and immovable properties, and proxy accounts opened in the names of various individuals without their knowledge or consent. The accused allegedly operated multiple benami accounts and fixed deposits through two cooperative credit societies. Large sums of cash were reportedly deposited into these accounts, converted into fixed deposits, and later withdrawn in cash. The investigation further found that the accused controlled such

accounts using his own mobile number and nominee information, and that he allegedly used the proceeds of crime to acquire movable and immovable property.

Source: Directorate Of Enforcement

A Sydney couple accused in multimillion dollar bank fraud

Australian police have charged a Sydney couple over their alleged involvement in a large-scale bank fraud scheme that reportedly caused losses exceeding AUD 40 million. According to investigators, the man, who worked in the banking sector, allegedly used his position to help approve fraudulent loan applications and mortgage documents. Police claim the scheme involved obtaining millions of dollars in home, business, and vehicle loans through false information and forged documents. Police have already charged numerous individuals and restrained millions of dollars in assets linked to the alleged scheme. Both accused have been refused bail and are expected to face court proceedings as investigations continue.

Source: The Sydney Morning Herald

REGULATORY UPDATE

FINMA Annual Report 2025: Money Laundering Supervision

By Neha Treesa Joy

According to its 2025 Annual Report, combating money laundering remained an important supervisory priority for FINMA (Swiss Financial Market Supervisory Authority). The report highlights that FINMA continued to focus on business conduct risks, including money laundering, sanctions compliance, and governance weaknesses, with the aim of protecting the integrity of Switzerland's financial system.

Under Article 25 of the Anti-Money Laundering Ordinance-FINMA (AMLO-FINMA), Swiss financial institutions are required to conduct a documented money laundering risk

analysis based on their business activities, products, and client relationships. FINMA identified gaps in how some institutions assessed inherent risks. Risk mitigation measures and institution-specific risk tolerance were incorrectly considered when evaluating inherent risk, resulting in high-risk factors such as foreign politically exposed persons (PEPs) and complex cross-border trust structures being classified as medium rather than high risk.

The regulator also noted that institutions often lacked sufficient detail in their risk analyses. Institutions with higher risk tolerance shall provide more granular assessments of individual risk factors, including country-specific risk exposure.

FINMA emphasised preventive supervision and conducted supervisory reviews to identify weaknesses in risk management and control frameworks. These reviews identified weaknesses in due diligence, transaction monitoring and reporting of suspected money laundering. FINMA, thus, recommends the adoption of a strong compliance culture along with review of all business relationships.

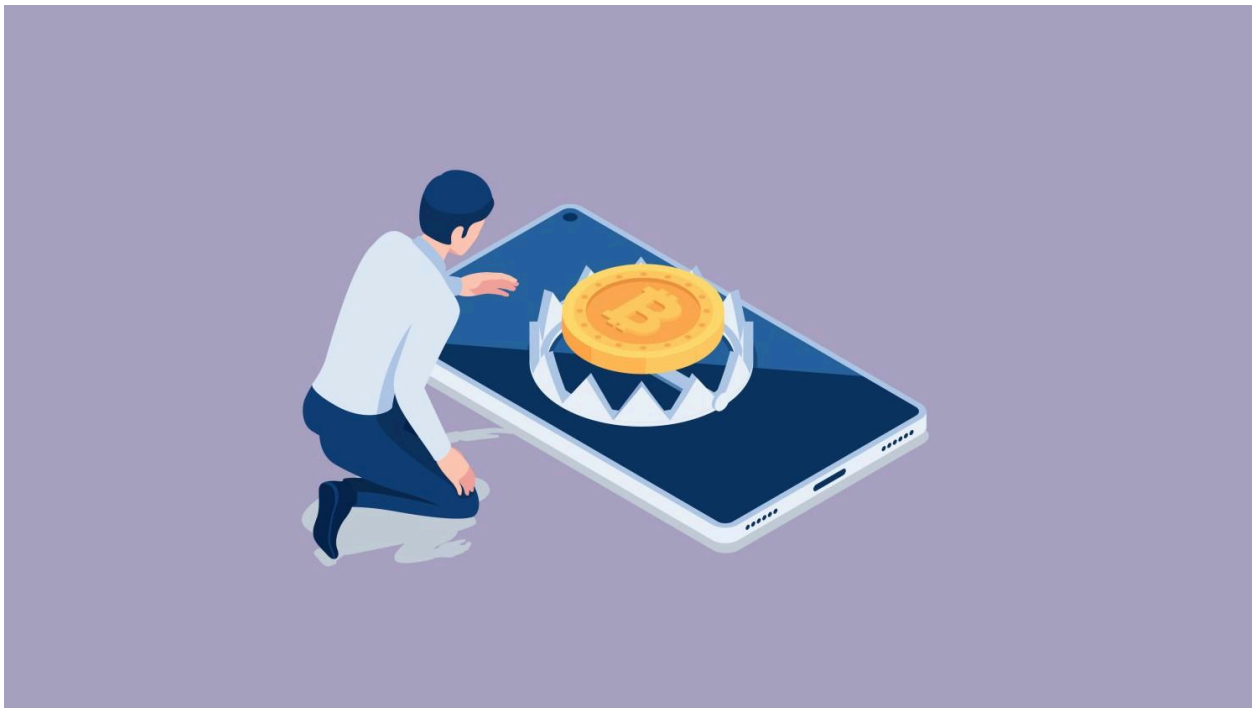
The report also highlighted emerging risks, including those associated with digitalisation and crypto-related activities, which are considered vulnerable to misuse for financial crime and money laundering.

Enforcement remained a key tool in addressing anti-money laundering deficiencies. FINMA reported numerous enforcement proceedings and interventions where institutions failed to meet supervisory expectations or comply with regulatory obligations. The Annual Report demonstrates FINMA's continued focus on strengthening anti-money laundering controls, improving governance standards, and ensuring that supervised institutions effectively manage financial crime risks.

Source: FINMA

Internet Crime Report 2025: Key findings on cryptocurrency fraud

By Adhila Thirumalai



According to the FBI's(Federal Bureau of Investigation) Internet Crime Complaint Centre (IC3), cyber-enabled fraud accounted for nearly 85% of all reported losses in 2025. During the year, the FBI received 1,008,597 complaints reporting $20.877 billion in losses, up from 860,000 complaints and $16.6 billion in losses recorded in 2024.

Key Trends

The top five types of internet crime by loss were investment fraud, Business Email Compromises (BEC), tech support, romance scams, and government impersonation. Among these, investment fraud generated the highest financial loss of $8.65 billion. Analysis of transaction information reported to IC3 revealed that cryptocurrency investment fraud alone reported the largest source of financial losses to Americans in 2025, with $ 7.2 billion. Compared with 2024, cryptocurrency fraud losses increased by 24%, highlighting its evolution towards mainstream financial fraud.

Typologies of cryptocurrency fraud

Scammers first establish contact via text messages, social media sites, ads, or dating apps before quickly moving the conversation to a messaging platform. Victims are then introduced to investment organisations posing as expert industry insiders, providing advice on trading or investing in bitcoin or gold. Victims send cryptocurrencies to fake investment fraud platforms or apps, where they are provided fake earnings and loans to promote further investments.

When the victims attempt to withdraw their money, additional charges are imposed under the guise of taxes and fees as a final attempt to extract money before the scammers flee with all of the victims' money. Victims are also often targeted in recovery scams that promise to assist them in recovering their lost funds. 3,780 victims of cryptocurrency investment fraud were contacted, with 78% of them unaware they were being duped.

AI-enabled techniques in fraud schemes

Artificial intelligence (AI) is being used by fraudsters to make their scams more scalable and convincing. AI enables scammers to engage with thousands of potential victims simultaneously. Fraudsters also impersonate as celebrities, business executives, and other trusted figures using deepfake technology, voice cloning, and AI-generated videos.

Social media platforms are frequently used to promote these false endorsements, making scams seem more legitimate and more difficult for victims to identify.

IC3 data further highlights this trend, reporting 7,623 AI-related cryptocurrency fraud complaints and corresponding losses of nearly $658.7 million in 2025. Cryptocurrency's speed, global accessibility, and complex transaction reversibility make it particularly attractive to fraudsters seeking to move and conceal illicit proceeds.

The IC3 findings demonstrate that the convergence of social engineering techniques, AI-enabled deceptions and fast moving cryptocurrency payment systems has significantly increased both the scale and sophistication of such frauds. As fraudsters continue to utilise new technology, due diligence and awareness of investment offerings are crucial for avoiding financial losses.

Source: FBI Internet Crime Report 2025

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.