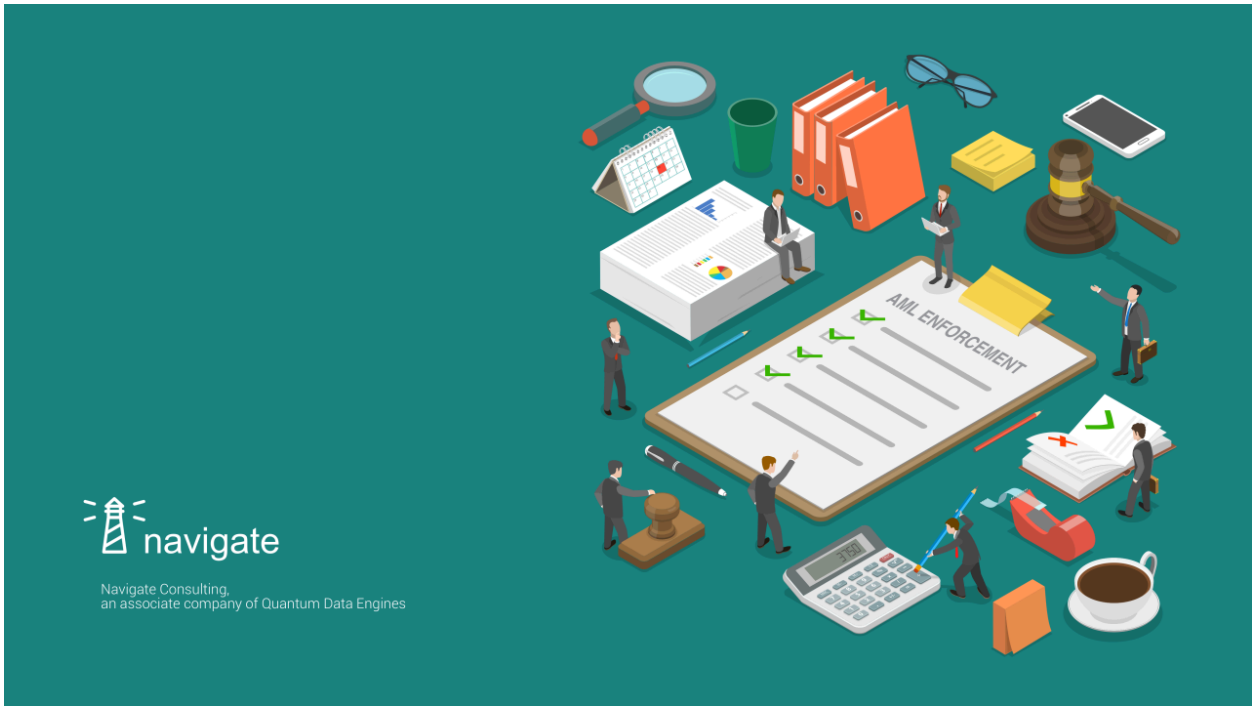

Lessons from AML Enforcement Actions in 2025| UAE introduces new AML regulations| MSBs as financial channels in drug trafficking and more

January, 2026

Lessons from AML Enforcement Actions in 2025

By Shivani S.

In 2025, regulatory action intensified due to mutual evaluations and the introduction of new AML regulatory requirements across regions and financial institutions.

Businesses operating in higher-risk sectors faced increasing pressure to improve internal controls and risk management frameworks to meet regulatory expectations. Regulators are no longer limiting their focus to traditional banking institutions; fintechs, crypto firms, payment service providers, and other non-bank financial institutions have also been subject to penalties for AML control deficiencies.

International banks experienced scrutiny from host-country regulators due to failure to comply with local AML laws. Regulators focused not only on whether institutions had AML frameworks in place, but on whether those frameworks were effective, well-governed, and in line with their risk exposure.

Some key enforcement actions in 2025 include:

- The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) imposed the largest penalty in Canadian history against a virtual asset service provider.
- U.S authorities levied one of the highest penalties exceeding USD 500 million.
- The Singapore regulator took action against 9 financial institutions for AML failures linked to one money laundering case.

Common deficiencies identified:

- KYC procedures: Regulators identified failures to verify customer identity, understand ownership structures, and conduct ongoing reviews. Institutions were also found to have inconsistently applied enhanced due diligence measures to high-risk customers.
- STR filing: Deficiencies were found in regulatory reporting, including delays in STR filings and failures to escalate high-risk activity in time, thereby undermining the effectiveness of financial intelligence processes to detect illicit activity at an early stage.

- Governance: Governance shortcomings were frequently identified, such as a lack of senior management engagement and inadequate AML policies and procedures.
- AML Risk Assessments: Many institutions relied on risk assessments that did not reflect changes in customer profiles, business activities, delivery channels, or geographic risk.
- Transaction monitoring: A common deficiency involved transaction monitoring systems that generated high alert volumes but failed to identify genuinely suspicious activity. Enforcement findings cited poor scenario tuning and alert handling.

Thus, regulators expect institutions to demonstrate clear ownership of AML risks at the board level, with controls in place to update risk assessments. Organisations are also expected to test and validate AML systems to ensure timely mitigation of known weaknesses before they lead to regulatory action.

Financial institutions can meet these expectations by taking a risk-based approach to strengthen their AML frameworks. This includes regularly updating enterprise-wide risk assessments, ensuring timely regulatory reporting in their prescribed formats, and implementing and reviewing transaction monitoring systems.

The enforcement trends in 2025 emphasise the need for all sectors to have comprehensive AML policies and procedures in place that are tailored to their institution. Further, it is essential for institutions operating across jurisdictions to have a clear understanding of local AML regulatory requirements and apply consistent standards.

NEWS SNIPS FROM AROUND THE WORLD

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

FRI helps prevent ₹660 crore worth of cyber fraud losses

India's Financial Fraud Risk Indicator (FRI), launched on 22 May 2025 has played a significant role in protecting the digital financial ecosystem by helping to prevent cyber fraud losses of about ₹660 crore within six months of its introduction, according to the Department of Telecommunications (DoT). Supported by the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI), the system has been adopted by over 1,000 entities, including various banks and fintech partners. Reports indicate that many potentially fraudulent transactions have been blocked or issued alerts using FRI data, contributing to substantial loss prevention across the banking and digital payments landscape.

Source: The Hindu

Drug trafficker convicted for money laundering under PMLA

A criminal was convicted in Jalandhar for money laundering linked to cross-border drug trafficking activities. Initially found guilty for drug trafficking, investigations later revealed that the criminal played an active role not only in trafficking narcotics but also in managing and retaining the illicit proceeds derived from these activities. Cash generated from drug sales was accumulated and stored, enabling the laundering of criminal proceeds. Searches conducted under PMLA provisions led to the seizure and attachment of movable assets worth Rs 17 lakh.

Source: The Times of India

Swiss prosecutors indict Credit Suisse over compliance failures in Mozambique tuna bonds scandal

The Office of the Attorney General of Switzerland (OAG) has filed an indictment against a former Credit Suisse (CS) employee on charges of money laundering related to loans granted to Mozambican state-owned companies. The case involves more than $2 billion in loans extended by Credit Suisse to state-owned enterprises in Mozambique and the bank's business relationship with a foreign company. Approximately $7.9 million was allegedly transferred from Mozambique's Ministry of Finance to accounts held by that company at Credit Suisse in Switzerland. The indictment centres on Credit Suisse's termination of the commercial relationship and the subsequent transfer of funds abroad that were suspected to be of criminal origin, without the bank submitting a suspicious activity report to the Money Laundering Reporting Office Switzerland (MROS), despite the employee's knowledge of the circumstances.

Source: Swiss Federal Department

FCA fines Nationwide for failings in financial crime controls

The UK's Financial Conduct Authority (FCA) has imposed a £44.08 million fine on Nationwide Building Society for shortcomings in its financial crime systems and controls. The regulator found that Nationwide's due diligence and transaction monitoring were ineffective, leaving it unable to properly identify, assess, monitor, or manage money-laundering risks among its personal current account customers. Nationwide was unable to effectively identify, assess, monitor, or manage the money laundering risks among its personal current account customers and did not have accurate information about its high-risk customers. Nationwide was aware of the weakness in their systems but failed to address them in time.

Source: FCA

Europol dismantles illegal gambling and money laundering network

A major cross-border law enforcement operation has disrupted a violent criminal network behind extensive illegal gambling and money laundering activities in Sweden and Spain. According to Europol, the network used violence to enforce debts and maintain control over sections of the Stockholm gambling market and was linked to drug trafficking across the Nordic region, highlighting the interconnected nature of organised crime across borders. The coordinated strikes, conducted between 28 and 29 November, involved nearly 150 police officers who searched multiple locations, resulting in the arrest of five key suspects.

Source: EUROPOL

REGULATORY UPDATE

UAE introduces new AML regulations

By Neha Treesa Joy

The UAE has strengthened its AML/CFT framework by introducing new predicate offences and broadening the scope of existing ones to respond to emerging financial crime risks. This includes criminalisation of proliferation financing, reflecting international security concerns and FATF expectations.

The UAE has significantly broadened the definition of predicate offences for money laundering to cover a wider range of underlying crimes. These now include tax evasion, cybercrime, terrorism financing, proliferation financing, and offences involving digital systems and virtual assets.

They also lowered the legal threshold for establishing principal AML/CFT offences under its enhanced regulatory framework. The new law allows authorities to establish liability not only where actual knowledge is proven, but also where sufficient or circumstantial evidence demonstrates that a person knew or should have known of the illicit nature of the funds or activity. This represents a significant shift from earlier requirements that relied heavily on direct proof of intent.

Penalties for crimes such as money laundering, proliferation financing and terrorist financing have increased, where legal entities can be fined between 5 million AED to 100 million AED or an amount equivalent to the property involved.

The Financial Intelligence Unit's powers have been expanded, allowing it to freeze assets, suspend suspicious transactions, and require timely reporting from regulated entities, while inter-agency cooperation across domestic regulators has been strengthened. UAE courts are now empowered to enforce foreign provisional measures and confiscation orders, enhancing both domestic enforcement and cross-border asset recovery.

The expansion of predicate offences under the UAE's enhanced AML/CFT framework marks a significant strengthening of the country's approach to combating financial crime. By widening the range of underlying offences, including tax evasion, cybercrime, virtual asset–related crimes, terrorism financing, and proliferation financing, the UAE has closed key legal gaps and aligned more closely with FATF standards.

Source: UAE Legislation

DOMAIN MATTERS

Money Service Businesses (MSBs) as Financial Channels in Fentanyl Trafficking

By Adhila Thirumalai

INTRODUCTION

According to the United States Drug Enforcement Administration (DEA), Fentanyl is a synthetic opioid typically used to treat severe pain and is classified as a Schedule II controlled substance that is approximately 100 times stronger than morphine, presenting significant public health and national security concerns.

In December 2025, U.S. policymakers publicly declared illicit fentanyl and its core precursors as a weapon of mass destruction, reflecting the growing concerns over its societal impact and the role of transnational criminal networks.

Fentanyl trafficking operates through complex, cross-border supply chains. The chemical precursors, primarily sourced from China, often advertised with specific code names on darknet platforms, are used to manufacture illicit fentanyl in foreign clandestine labs. These finished products/drugs are further smuggled into the United States through Mexico. Illicit fentanyl is frequently mixed with other drugs to increase the potency of the drug, sold as powders and nasal sprays, and increasingly pressed into pills made to look like legitimate prescription opioids.

The FinCEN (Financial Crimes Enforcement Network), through its 2019 advisory, identified new trends, typologies, and red flags of suspicious activities linked to the procurement of fentanyl precursor chemicals by Mexico-based Transnational Criminal Organizations (TCOs). The advisory highlighted the various financial mechanisms enabling the illicit fentanyl trade. Those mechanisms include the use of shell companies, money transfers through banks, Money Services Businesses (MSBs), online payment processors, and transactions using virtual currencies.

The recent Financial Trend Analysis 2025 report indicates that 32% fentanyl related Suspicious Activity Reports (SARs) showcase that Money Services Businesses (MSBs) are significant financial channels for the financial flow of illicit fentanyl trade.

WHAT ARE MONEY SERVICE BUSINESS (MSB)?

According to FinCEN, the term "money services business" includes any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

1. Currency dealer or exchanger.
2. Check casher.
3. Issuer of traveller's checks, money orders or stored value.
4. Seller or redeemer of traveller's checks, money orders or stored value.
5. Money transmitter.
6. U.S. Postal Service.

Among these, currency exchangers and money transmitters represent the highest exposure to fentanyl related financial activity due to their speed, agent-based models and cross-border reach.

WHY ARE MSBs USED IN TRAFFICKING FENTANYL?

According to FinCEN 2024, MSBs are frequently used to finance various stages of the fentanyl supply chain, from the procurement of precursors, transportation, to settlement between trafficking networks. The cross–border nature of fentanyl trade subjects traffickers to several enforcement and regulatory regimes, increasing their reliance on MSBs to move funds. Criminals choose speed over stability, thus, illicit supply chains prioritise rapid settlements of funds, minimum exposure to avoid any trace. MSBs remain an attractive financial channel for illicit financial flow as they provide accessibility, convenience and specialization.

TYPOLOGIES OF ILLICIT FENTANYL TRADE USING MSBs

- Money transfer through MSBs: MSBs are frequently used to transfer money from Mexico or US via Hong Kong or other countries to individuals, shell and front companies associated with either People's Republic of China (PRC) based supplier or chemical broker. While some money transfers are sent directly from Transnational Criminal

Organizations (TCOs) in Mexico to PRC-based suppliers, many of these foreign transactions are cleared in U.S. dollars through U.S. correspondent banks and Mexico- and PRC-based agents of the U.S. MSBs.

- Structured MSBs: US-based MSBs structure the money transfer to Mexico through multiple agents and beneficiaries to evade BSA reporting. The structuring involves keeping the money transfer below the threshold to avoid identification and reporting requirements.
- High-volume transfers to apparently unrelated beneficiaries: A single U.S. remitter sends numerous payments to different foreign individuals who appear unrelated but are operationally connected. In many cases, beneficiaries share the same phone number or email address, and the contact information is linked to pharmaceutical or chemical sales websites.

CONCLUSION

MSBs and their banking partners are more vulnerable to financial flows associated with drug trafficking since fentanyl supply chains depend more on third-country intermediaries, indirect payment routes, and structured transactions. To identify and stop fentanyl-related illicit funding, financial institutions need to improve risk-based controls, implement targeted transaction monitoring, and information sharing.

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.

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