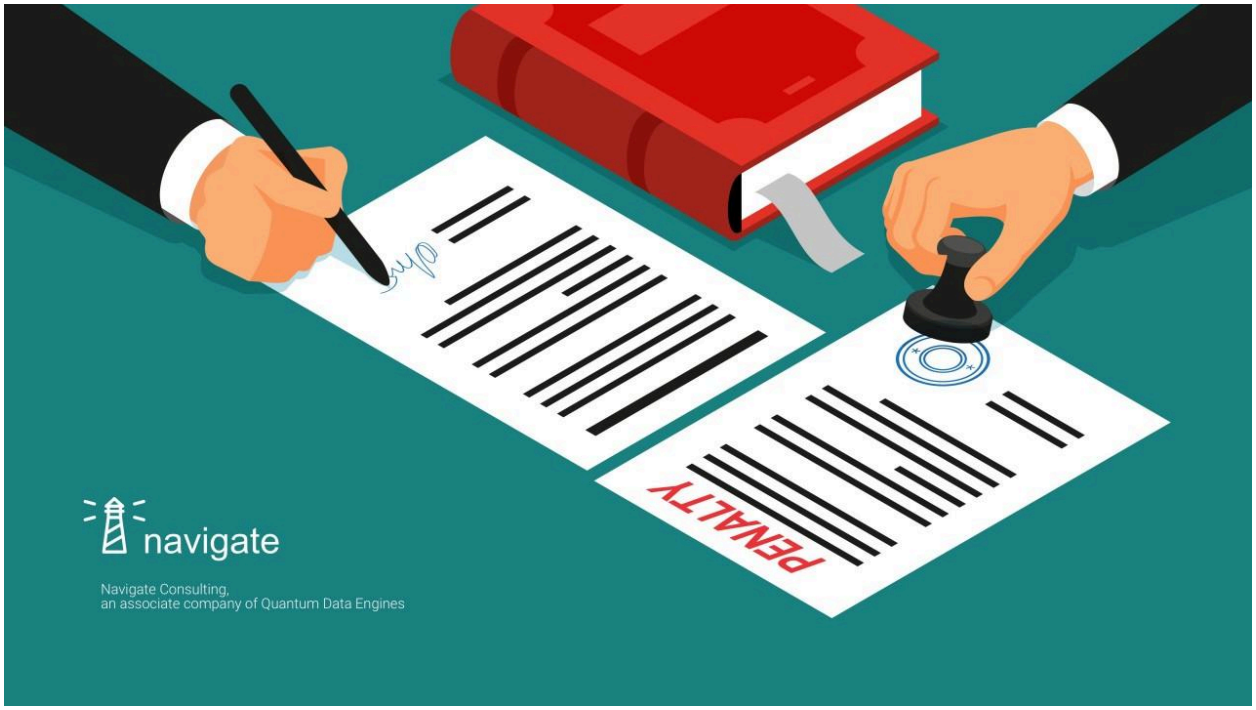

The Laundry Times August Edition | Singapore regulator takes action on 2023 money laundering case | Terrorism Financing typologies and more

August, 2025

TOP STORY

Singapore takes regulatory action against financial institutions for 2023 money laundering case

By Shivani S.

The Monetary Authority of Singapore (MAS) has imposed financial penalties totalling $21.5 million on six banks and three other financial institutions (FIs) for breaches related to Singapore's largest money laundering case to date.

This enforcement action follows the high-profile 2023 money laundering scandal, where authorities seized more than $2.2 billion in illicit assets and arrested 10 foreign nationals during coordinated raids in August 2023. The criminals held money gained from online gambling operations and overseas scams in bank accounts in Singapore, and converted some of their cash into real estate, cars, handbags, and jewellery. The case highlighted critical vulnerabilities in the financial sector's defense against money laundering.

According to the MAS, while most of the penalised institutions had formal anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks in place, the deficiencies largely came from the weak implementation of existing controls. These lapses allowed several high-risk individuals to take advantage of gaps in due diligence and monitoring processes.

Institutions failed to meet regulatory expectations in the following areas:

- Customer risk assessment: Money laundering risk ratings were inadequately calculated for certain customers. This misclassification affected their ability to apply appropriate risk mitigation measures, particularly for persons of interest (POIs) involved in the scandal.
- Source of wealth verification: All nine institutions failed to sufficiently verify the source of wealth of high-risk customers. In several cases, red flags in documentation were either overlooked or inadequately followed up, and some institutions did not verify key aspects of the declared wealth, which is an integral step when dealing with increased ML risks.

- Transaction monitoring: Institutions failed to properly investigate transactions flagged by their monitoring systems. These transactions were often unusually large or inconsistent with the customer profiles, indicating potentially suspicious activity that required deeper investigation.
- Post-STR follow-up: Two institutions were found to have failed to implement timely risk mitigation measures even after filing STRs. There was a delay in taking necessary actions such as reclassifying customer risk levels or conducting enhanced monitoring.

In addition, MAS has taken actions against relationship managers (RMs) who were involved in managing the FIs' relationships with the POIs. They failed to develop and implement proper policies for source of wealth verification, customer risk assessment, name screening, and ongoing customer due diligence (CDD) reviews.

MAS has also recently revised its AML/CFT guidelines due to emerging risks and the findings from such supervisory reviews. Financial institutions must file STRs within five business days after suspicion has been established and not later than one business day for cases involving sanctioned parties. Thus, institutions are expected to apply rigorous and proportionate controls, especially when dealing with high-risk customers.

This case highlights that policy frameworks being in place alone are not sufficient. The effectiveness of AML/CFT compliance depends on the consistent execution of those policies. MAS expects all financial institutions to benchmark their practices with supervisory standards and industry best practices. Institutions must execute robust and risk-based measures to prevent money laundering. Lastly, relationship managers, as the first line of defence, must identify red flags and escalate concerns quickly to ensure timely risk mitigation.

Source: Monetary Authority of Singapore

NEWS SNIPS AROUND THE WORLD

Hong Kong police arrest 82 suspects and seize assets linked to a criminal syndicate

Hong Kong police have arrested 82 individuals, including a 44-year-old mastermind, in a major citywide anti-transnational crime operation targeting a syndicate that laundered nearly HK$40 billion (US$5.1 billion). The group used a trust company set up in 2021 to carry out money laundering disguised as legitimate trade. HK$39.6 billion was transferred through shell companies to mule accounts, cryptocurrency platforms, or used to pay off personal credit card loans and buy luxury goods. Police raided multiple locations, seized over HK$15 million in assets, and froze HK$1.13 billion in suspected criminal proceeds. Items confiscated included 11,000 wine bottles, luxury watches, gold, handbags, and a rare 1.6-metre Labubu doll valued at HK$1 million.

Source: South China Morning Post

Joint investigation exposes sophisticated ATM theft scheme

A joint investigation team between Romania and the United Kingdom, with the support of Eurojust and Europol, has dismantled a criminal network involved in large-scale ATM fraud across several European countries. The majority of the money was stolen in the UK by using a bank card to simulate a cash withdrawal at an ATM. The fraudsters would remove the ATM screen during the process, cancel the transaction, and then physically access the machine to grab the cash inside before the transaction was finalized. They also carried out card fraud by using software to detect card numbers, which they then exploited to generate illegal profits through fake transactions. Coordinated actions led to multiple arrests and searches, with law enforcement seizing luxury vehicles, real estate, electronic devices, and cash.

Source: EUROJUST

India’s cybercrime losses cross ₹22,000 crore in 2024

The Ministry of Home Affairs in India stated that India lost Rs 22,845.73 crore to cyber criminals in 2024, marking a sharp 206 percent surge from the money lost in 2023. The cited data was taken from the National Cyber Crime reporting portal (NCRP) and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), both operated by the Indian Cyber Crime Coordination Centre (I4C). With the help of the CFCFRMS, the government was able to prevent and recover Rs 5,489 crore from fraudsters. A suspect registry, launched in September 2024 in collaboration with banks and financial institutions,

has helped in identifying 11 lakh fraud suspects and flagged more than 24 lakh mule accounts.

Source: Times of India

China implements new AML rules for precious metals and gemstone dealers

China's central bank, the People's Bank of China (PBOC), has implemented new AML/CFT regulations for precious metals and gemstone dealers. The rules are applicable from August 1st to all legally operating dealers involved in the trading of precious metals like gold, silver, and platinum, as well as gemstones such as diamonds and jade. Dealers are now required to report any single or cumulative daily cash transactions of 100,000 yuan (approximately 13,977$) or more, including foreign currency equivalents. These transactions must be reported to the China Anti-Money Laundering Monitoring and Analysis Center within five working days.

Source: State Council of China

Cybercrime police arrest 45 in major online fraud crackdown

The Hyderabad Cybercrime Police arrested 45 individuals linked to 25 cases of online fraud. The arrested individuals were involved in various types of scams, including trading frauds, voice phishing, fake job offers, digital arrest scams, customer care frauds, and

matrimony-related frauds. The police seized multiple devices, including laptops, mobile phones, SIM cards, and banking documents. Hyderabad Police succeeded in securing 153 refund orders from the court in 40 cases, amounting to ₹99.14 lakh, to be returned to the victims.

Source: The Hindu

Rs. 3.24 crore laundered through cryptocurrency

The Telangana Cyber Security Bureau (TGCSB) arrested three individuals for laundering money from a cyber fraud case by converting it into cryptocurrency and sending it to fraudsters abroad. A victim reported losing Rs 3.24 crore between May 30 and July 9 after being misled through a WhatsApp group that shared fake stock market updates. The funds were first routed to a mule account and later transferred to another account for withdrawal. The withdrawn cash was then converted into cryptocurrency (USDT) via a crypto wallet. A Telegram group, suspected to be run by Chinese nationals, offered high commissions for converting cash into cryptocurrency, which encouraged one of the accused to recruit others to open multiple bank accounts.

Source: The Indian Express

REGULATORY UPDATE

Singapore revises AML/CFT notices

By Anna Paulin

The monetary authority of Singapore (MAS) has published revised AML/CFT notices and guidelines imposed on financial institutions (FIs) and variable capital companies (VCCs). The revised amendments ensure that Singapore's Anti Money Laundering (AML) and countering financing of terrorism (CFT) regime remains clear and aligned with international standards. The amended regulation has been drawn from the latest revised Standards set by the Financial Action Task Force (FATF), the global standard-setter for measures to combat ML, TF, and Proliferation Financing (PF). MAS has enacted revised AML/CFT Notices effective from 1 July 2025.

- Proliferation Financing (PF) Risk Assessment: As an outcome of the MAS's focus to be in line with the revised FATF standards, MAS has amended the regulations to ensure that ML risks include PF risks. It requires FIs and VCCs to carry out PF risk assessment on a standalone basis or while conducting ML/TF risk assessments. MAS stated in its response that PF risk assessments should be done as soon as possible if they are not already being carried out.
- Beneficial Owner Identification: To identify beneficial owners (BO), FIs and VCCs need to verify the identities of the BO using relevant and reliable data. In situations where there is a chain of ownership or control, FIs and VCCs will have to identify the legal persons or legal arrangements along the chain of ownership or control.
- Source of Wealth (SoW) Verification: In cases involving higher-risk Trust Relevant Parties (TRPs), a trust company must carry out enhanced customer due diligence when engaging in business with any TRP identified as higher risk for ML/TF. SoW due diligence should be carried out on such higher-risk TRPs when they provide assets to the legal structure. MAS also states that for customers where SoW establishment is a requirement, FIs and VCCs may adopt a risk-based approach for documentation. As part of this process, when gifts or assets from third parties make up a significant part of a customer's wealth, FIs and VCCs must verify that these gifts or assets are legitimate.
- Expectations on STRs and Screening Tools: MAS expects FIs and VCCs to have appropriate frameworks in place to ensure that investigations are completed on time, and cases involving higher ML/TF risk concerns are prioritised. The amendment also guides FIs and VCCs to address gaps in existing screening tools. These enhancements should follow a risk-based approach. Moreover, FIs and VCCs should assess whether the vendor solutions they rely on for screening are adequate and enable them to be alert to material ML/TF risk concerns.

These revisions reinforce Singapore's commitment to global AML/CFT standards, and FIs/VCCs must take timely steps to implement the changes effectively.

Source: Monetary Authority of Singapore

DOMAIN MATTERS

Abuse of traditional financial services in terrorism financing

By Neha Treesa Joy

Terrorist financing continues to pose a serious threat to global security, as terrorist groups evolve their methods to exploit both traditional and emerging financial systems. In response to these growing challenges, the Financial Action Task Force (FATF) recently released its Comprehensive Update on Terrorist Financing Risks Report. The report provides a detailed assessment of how terrorists raise, move, and use funds across various regions and sectors.

The following section highlights specific ways in which traditional banking channels, particularly deposit accounts, wire transfers, and cards, are being abused for terrorist financing purposes.

- Deposit Accounts: Terrorists sometimes use deposit accounts for fund storage, although less often than cash. These accounts are often in the names of third parties or shell companies and may be opened in other jurisdictions to hide the true owner. Small terrorist cells or lone actors may use personal deposit accounts with low, legally sourced balances to avoid detection.
- Wire Transfers: Wire transfers continue to be used for cross-border terrorist financing, although they are less common compared to informal channels like hawala. These transfers usually involve relatively small amounts, often below USD 10,000, and are typically limited to one or two transactions. Domestically, wire transfers are also utilized to circulate money among group members.
- Credit and Debit Cards: Cards are often used by individual terrorists or small cells. Some EU-based supporters of Al-Qaeda used credit cards linked to foreign bank accounts to purchase virtual assets for donations. Compared to wire transfers, cards may offer less transparency, particularly when disguised as commercial payments. Credit cards can fund daily expenses from legitimate income or can be used through front organisations like NPOs or companies.
- Fraudulent Use of Cards: Some cases involve the use of fake documentation to obtain credit cards from other countries. These cards are used to purchase items like phones and tech devices, which are then either distributed or sold to fund operational expenses like document forging, residency applications, and recruitment. Prepaid cards are attractive to terrorists due to their anonymity and flexibility. They can be preloaded, used at ATMs globally, and accepted by a wide range of merchants. One major concern is that these cards are often poorly regulated across different countries, can be loaded remotely, transported, and traded easily across borders, and are often distributed by vendors with inconsistent KYC or proper due diligence.

While terrorist groups are shifting towards more anonymous and informal financial methods, traditional financial services, banks, cards, loans, and prepaid products are still exploited, especially by individuals and small groups. Gaps in regulation, inconsistent international cooperation, and emerging platforms like neobanks and prepaid cards represent ongoing vulnerabilities that need stronger regulation and cooperation.

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.