Strengthening Financial Institutions' (FIs) Countering the Financing of Terrorism (CFT) Controls

May 2023

Strengthening CFT controls in FIs

As an international financial center and transport hub, Singapore is vulnerable to being a node for illicit financing, including the raising, moving and transfer of funds (including virtual assets) to support terrorism or terrorism financing (TF) activities.

FIs need to remain vigilant to these risks and implement robust controls at key stages of the account lifecycle, including at on-boarding and ongoing monitoring.

MAS conducted an industry-wide survey of CFT-related controls, and followed up with a series of thematic reviews to assess FIs' TF risk understanding and examine the effectiveness of their CFT-related controls. This paper sets out MAS' key observations, and highlights our supervisory expectations that FIs should review against their own controls.

Note: The paper does not impose new regulatory obligations. However, FIs should benchmark themselves against the practices and supervisory expectations set out in this paper in a risk-based and proportionate manner, and conduct a gap analysis. In doing so, FIs should give due regard to the risk profile of their business activities and customers. Where FIs observe any gaps in their frameworks and controls, specific remediation/enhancement measures should be identified and implemented in a timely manner.

SG SINGAPORE

Key requirements and expectations on CFT

Terrorism (Suppression of Financing) Act (TSOFA)

- FIs are prohibited from dealing/transacting with individuals and entities which are:
  - Designated by the UN Security Council (e.g. those persons in the ISIL (Da'esh) and Al-Qaida Sanctions List)
  - Listed in the First Schedule to the TSOFA or identified within information provided by the authorities

  unless an exemption order has been issued by MHA.
- FIs should have robust processes in place to detect such individuals and entities, and should **immediately freeze** any assets related to these persons.
- FIs should also disclose any information about such assets by reporting to Police (e.g. through the prompt filing of a suspicious transaction report (STR)).

Key expectations on FIs' CFT controls

- FIs should ensure that **existing AML/CFT frameworks and processes enable effective compliance with the TSOFA, CDSA and relevant MAS' rules.**
- **FIs should be aware of the external TF risk environment**, including geographies with heightened TF risks, emerging typologies and common payment methods used.
- **FIs should implement adequate controls to mitigate TF risks**, taking into account the extent of their TF risk exposure, including the size of their business, nature and complexity of their business model or transactions, as well as the geographical base of their customers.
- **FIs should subscribe to MAS' website[1] to be alerted promptly to changes to the lists of UN-designated individuals and entities.**

[1] https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions

Maintain awareness of TF threats and vulnerabilities

TF Threats

- As set out in Singapore's TF National Risk Assessment Report (NRA)[2], Singapore is **vulnerable to the TF threat of raising and moving of funds in support of terrorists/terrorist organisations/terrorist activities overseas.**
- **Radicalised individuals** continue to pose a salient TF threat to Singapore.
- Other than existing TF threats posed by the Islamic State of Iraq and Syria (ISIS), Al-Qaeda (AQ) and Jemaah Islamiyah (JI), **FIs should be aware of the external TF environment, and be vigilant against potential financing of other existing or new terrorist groups regionally and globally.**
- FIs are also reminded of new and emerging international typologies in which TF can be financed, including through ransomware[3], arts and antiquities[4], and online crowdfunding mechanisms.

TF Vulnerabilities

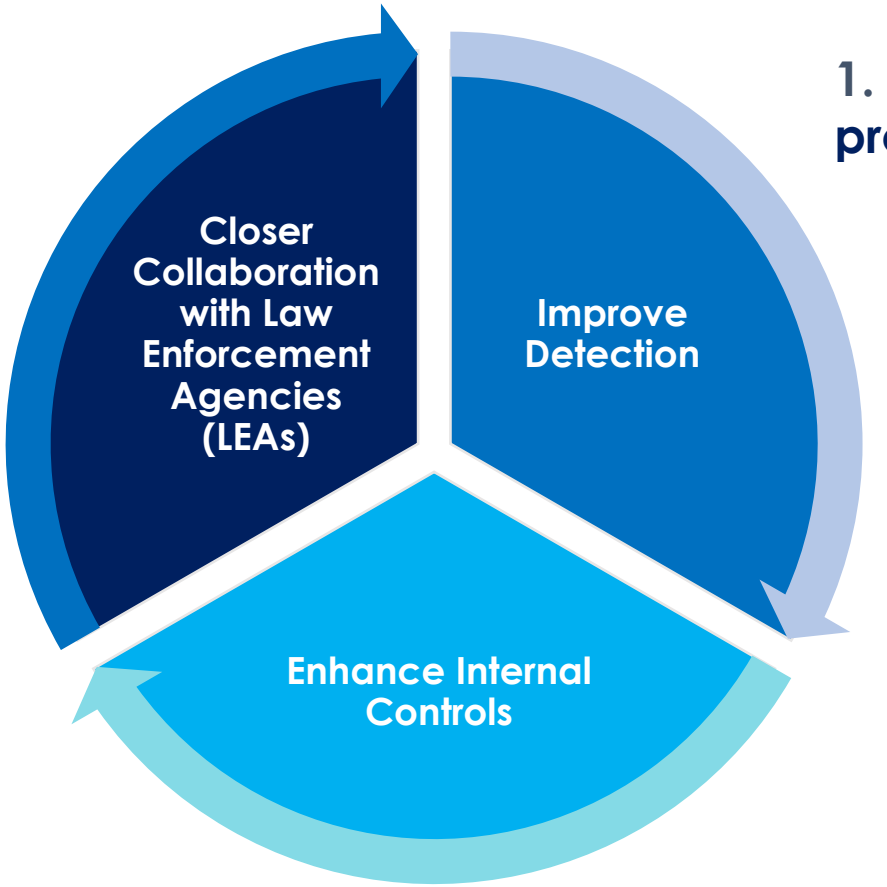
- **Money remittance services (or cross-border money transfer services) and banks are inherently more vulnerable to TF threats**, given the relative ease with which their services may be accessed, coupled with Singapore's connectivity as a financial and transport hub, and proximity to countries exposed to terrorist activities.
- **Digital payment token service providers, precious stone and metals dealers, and non-profit organisations** were also identified as sectors that are more susceptible to TF.
- **International typologies have shown that virtual assets, for example digital payment tokens (DPTs)**, have been used to support terrorist activities. DPTs are susceptible to TF abuse because of the pseudonymity they offer, their convenience as a near-instantaneous value transfer medium, and the cross-border nature of the transactions. DPT risks are increased when the transactions concern jurisdictions which have yet to regulate and supervise DPT service providers.
    - Terrorists and their financiers may further exploit services such as mixers, tumblers and privacy coins to obfuscate their transaction flows.

[2] https://www.mas.gov.sg/publications/monographs-or-information-paper/2022/terrorism-financing-national-risk-assessment-2020. Details of our National Strategy for Countering the Financing of Terrorism are set out in https://www.mas.gov.sg/publications/monographs-or-information-paper/2022/national-strategy-for-countering-the-financing-of-terrorism.
[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing-Potential-Risk-Indicators.pdf.coredownload.pdf
[4] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.pdf.coredownload.pdf

Key areas for improvement

- MAS identified the following areas for improvement arising from our supervisory engagements:

1. Strengthening screening processes



2. Leveraging data analytics

3. Conducting regular reviews to strengthen internal controls and processes

4. Ensuring timely and quality STR submissions

1. Strengthening screening processes

FIs should review existing screening processes to ensure compliance with TSOFA, CDSA and MAS rules

- Screening is a basic preventive measure for FIs to detect potential TF threats. Weaknesses in FIs' screening processes can impede their ability to promptly detect TF threats, and take commensurate measures to address such risks.
- FIs should regularly review the adequacy and appropriateness (including frequency) of screening processes and checks to comply with TSOFA, CDSA and the relevant MAS rules. Immediate steps should be taken to address any weaknesses identified.
- FIs should subscribe to the MAS website[5] to get up-to-date information on changes to terrorist designation. FIs may also wish to subscribe to or check the UN website[6] regularly for updates.
- FIs can refer to MAS' Information Paper on Strengthening AML/CFT Name Screening Practices[7], which sets out recommended practices in relation to name screening frameworks and processes.

[5] https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities
[6] Please refer to the relevant UN webpages referenced in the link in footnote 5.
[7] https://www.mas.gov.sg/publications/monographs-or-information-paper/2022/strengthening-aml-cft-name-screening-practices

Case Studies: Weaknesses in screening processes

Case Study 1:

× As part of FI A's onboarding processes, newly onboarded customers were screened in batches within 24 hours of account creation. However, there were no specific controls on account transactions prior to the completion of screening checks. As such, customers were still allowed to transact on FI A's platform, including transferring funds to overseas wallets, even though they have not been screened.

× By allowing customers to perform transactions before the completion of screening checks, FI A is exposed to the risk of being a conduit for illicit financing, including TF.

× MAS expects FI A to implement controls to ensure that all customers are screened against the relevant lists as soon as is reasonably practicable after establishing business relations with them and before undertaking any transaction for the customer. This is necessary to mitigate the risk of inadvertent breaches of relevant laws and regulations relating to sanctioned parties.

Case Studies: Weaknesses in screening processes

Case Study 2:

- For customers who defaulted on existing loans with outstanding arrears, FI B no longer classified them as their existing customers and removed them from its core banking system.

- As a result, while FI B would still continue the debt recovery from these customers, these customers were no longer subjected to the FI's AML/CFT controls as well as ongoing screening checks which were performed on the core banking system. This exposed FI B to the risk of dealing with higher risk (or even sanctioned) customers within the bank without commensurate controls in place.

- Due to this gap, FI B subsequently unknowingly engaged in debt recovery with a prohibited person who was known to be involved in terrorist activities without performing the necessary risk mitigation-measures.

- FI B has since remediated this gap by ensuring that customers from all its business lines (including those on debt recovery schemes) are included in its core banking system and subjected to the requisite AML/CFT controls.

2. Leveraging data analytics

Leveraging data analytics to enhance TF detection

- Transactions involving TF (e.g. those in relation to self-radicalised persons) often involve small value amounts which may be difficult to distinguish from legitimate transactions.
- Relying on a single data source alone (e.g. from transaction monitoring) may not provide sufficient indication on whether any TF element is involved.
- To better identify behaviour potentially indicative of TF, some FIs have found it important to combine insights from multiple data sources, once a potential TF red flag is detected. To enrich their analysis, some FIs have also deployed more advanced methods such as network link analysis and geographical mapping of transactions involving higher-risk TF jurisdictions.

Combining insights from Multiple Data sources

- **Adverse News and Reports (e.g. from commercial databases)**
- **Transaction Monitoring**
- **Customer Due Diligence (CDD)**
- **Intelligence/Data from LEAs**

Leveraging more advanced methods to enhance TF detection

Network Link Analysis (NLA)

- Mapping out connected parties and transactional patterns after a suspected individual is picked up through a red flag

Targeted Geographical Tracking

- Analysis of remittance frequency and volume to higher risk corridors/jurisdictions
- Mapping out transactional patterns involving high-risk/conflict zones
- Monitoring of ATM withdrawal locations and log-in IP addresses

Case Studies: Enhancing TF detection using analytics

Case Study 1:

- FI C noted from adverse news that one of its customers was potentially linked to TF.
- FI C conducted transaction analysis on the customer and identified transaction patterns involving individuals in multiple higher TF risk jurisdictions. The transactions also involved multiple 3rd parties without apparent economic purpose.
- Through the use of network analysis, FI C identified a network of suspicious individuals linked to the customer. FI C promptly filed an STR on the network of individuals on potential TF concerns.

Case Study 2:

- FI D obtained a referral from a foreign authority that one of its customers was potentially linked to TF.
- FI D conducted transactional analysis on the individual and identified the following red flags:
  - Transactions occurring in higher TF risk jurisdictions
  - Attempts to conceal transactions to same individual by using multiple name variations
  - Apparent structuring of transactions to avoid reporting thresholds
- Through the use of network analysis, FI D identified a network of suspicious individuals linked to the customer and filed an STR on the network on potential TF concerns.

Case Study 3:

- FI E conducts network analysis on customers whose transactions involve all the following indicators:
  - Money Changers and Remittance Businesses (MCRBs)
  - Non-profit Organisations (NPOs)/crowd funding platforms
  - Higher TF risk jurisdictions
  - STR-linked parties
- Based on the analysis, FI E identified an individual with the following red flags:
  - Transactions involving multiple counterparties, some of whom are located in higher TF risk jurisdictions
  - Inflow of funds from an STR-linked individual with suspected TF nexus
  - Outflow of funds to an NPO located in a high risk jurisdiction
- FI E filed an STR on the individual on potential TF concerns.

3. Strengthening internal controls and processes on CFT

FIs should implement robust internal controls and processes to detect, escalate and mitigate TF risk identified during the customer account life-cycle

Maintain vigilance towards TF

- Enhance staff awareness of TF typologies and related red flags
- Strengthen staff competencies to pick up red flags from multiple sources that may indicate TF risk concerns
- Provide regular updates to senior management on the FIs' TF risk exposure

Establishing clear escalation channels on TF-related cases

- Institute clear internal processes to facilitate timely dissemination of information and escalation of hits on TF-related activity
- Put in place interim measures (e.g. temporary hold on accounts/transactions) while the FI is assessing potential TF risks

Timely Implementation of Risk Mitigation actions

- Conduct enhanced customer due diligence (ECDD) measures promptly where TF red flags are identified
- Implement assets/account freeze where the need arises, and conduct periodic checks to ensure that the freeze remains in place (and that there have been no unauthorised transactions)
- Timely filing of STRs and/or escalation to LEAs

4. Ensuring timely and quality STR submissions

Timely communication of TF observations through STR filings

- Effectively identifying and preventing TF requires close partnership between FIs and LEAs.
- As customer touchpoints, FIs would be able to observe behaviour indicative of TF, including new typologies, and financial products or payment methods susceptible to TF. FIs are encouraged to communicate such observations to LEAs, and file STRs in a timely manner.
- Where the FIs have additional information or useful insights relating to existing cases, they are encouraged to share such insights with LEAs, e.g. through the filing of supplementary STRs.
- Internally, FIs should continually enhance controls to address gaps identified from post mortem reviews of relevant TF-related cases and STRs, to strengthen FIs' on-going ability to detect potential TF risk concerns.

Case Study - Ensuring timely and quality STR submissions

- FI F adopts the following 3-pronged strategy as part of its investigation into TF-related activity:
  - **Analysis** – Reviewing subject entity's transactional and case history and conducting network link analysis to identify connected parties
  - **Risk mitigation** – Implementing mitigating controls, including ECDD measures, account freeze, etc.
  - **Information sharing** – Timely filing of STRs to share investigation outcomes with LEAs

- As part of the STR filing, FI F highlights observations uncovered during the course of investigation, including the typologies observed and new subjects identified which may be of interest to law enforcement.

- As and when FI F receives any material information relating to the identified network, it communicates such observations to the LEAs on a timely basis through the filing of supplementary STRs.

In Summary…

- MAS' thematic inspections showed that FIs have generally put in place the necessary frameworks and controls to detect and mitigate TF risks.
- FIs should assess the effectiveness of their controls against MAS' inspection findings and guidance provided here. Appropriate steps should be taken to address any gaps.
- FIs should continue to be alert to evolving TF risk and typologies, and ensure that effective controls, including screening checks, are in place to detect and mitigate these risk concerns. Particular attention should be placed on ensuring robust internal controls to escalate and mitigate TF risks. When relevant, STRs should be filed promptly and without delay.
- Senior management should be kept up-to-date on the FI's risk exposure, provide close oversight and maintain high risk management standards. MAS will continue to engage the FIs, including in the higher-risk money remittances and banking sectors, on on-going TF developments and risks.