



Common Deficiencies in Transaction Monitoring & Suspicious Transaction Reporting

Stewart McGlynn
Senior Manager (AML)
Anti-Money Laundering
Hong Kong Monetary Authority



HONG KONG MONETARY AUTHORITY
香港金融管理局



Financial Services and the Treasury Bureau
The Government of the Hong Kong Special Administrative Region



Disclaimer

- This presentation provides guidance to authorized institutions (“AIs”) on issues relating to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (“AMLO”) and the AMLO Guideline. The presentation is provided for training purposes and does not form part of the formal legal and regulatory requirements of the HKMA. It should not be substituted for seeking detailed advice on any specific case from an AI’s own professional adviser.
- The HKMA is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. These materials may be used for personal viewing purposes or for use within an AI. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the HKMA’s prior written consent.



Senior Management Oversight

- Senior management has an important role in the AI's AML/CFT systems
- Senior management should be satisfied that the AI's AML/CFT systems are capable of addressing the ML/TF risks identified





Role of Senior Management

- Section 23 of Schedule 2 - “Financial Institutions to prevent contravention of Part 2 or 3 of Schedule 2”
 - A financial institution must take all reasonable measures—
 - (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under Part 2 or 3 of this Schedule; and
 - (b) to mitigate money laundering and terrorist financing risks.
- Ultimate responsibility for ensuring the Bank’s systems are effective and comply with HKMA requirements rests with the Bank’s senior management (para 2.10-2.15 of AMLO Guideline)



Senior Management Oversight

- Should have committee designated for AML/CFT oversight
- Should have formal Terms of Reference
- Minutes of meetings – should show
 - fundamental and key AML/CFT control issues discussed in meetings
 - timely follow up on AML/CFT-related issues discussed in the last meeting
- Participation by management at sufficiently high level is needed



Transaction Monitoring

- Are the AIs transaction monitoring systems adequate, given their business activities and size? Are they used to support sanctions monitoring?
- How does the AI ensure systematic investigations into unusual transactions and potential STRs?





Risk Based Approach



Transaction Monitoring – MIS Reports

- Manual monitoring with MIS reports vs automated transaction monitoring system
- Type & Quality of MIS reports
 - To address Bank's Risks
- Parameters for MIS Reports
 - thresholds – Justification / Reasonableness
- Quality of Reviews
 - Bank should understand the transaction / pattern
- Adequacy & Timeliness of Compliance Reviews
 - Should have policy or procedure for regular review of adequacy and parameters



Transaction Monitoring System

- Alert handling
 - Should have sufficient justification / documentation
 - Should have adequate explanation for alert clearance (not just standard wordings)
 - Two level clearance / investigation
 - Staff awareness of alert scenarios
- Reference may be made to HKMA Circular B10/1C dated 4 July 2008



Name Screening Process

➤ Name matches / alerts

- It is for the AI to prove it has confirmed or eliminated a potential match (i.e. enhanced checking)
- Should have sufficient justification and documentation for alert clearance
- Quality of work performed
- Need to have P&P underpinning this important activity

➤ Updating of Database

- Need to have clear P&P – maintenance process needs to be codified
- Random checks to ensure accuracy

➤ Consistency – Practice versus P&P

➤ Where new methodology is employed

- clean up exercise on existing customer base required



Transactions with high-risk jurisdictions

- High-risk jurisdictions includes those sanctioned by the UN, *but may* also include others like jurisdictions which insufficiently apply FATF standards etc.
- What is the handling requirement for hits
 - Need to have P&P in handling transactions involving high-risk jurisdictions
 - Experience based response not acceptable
 - Need explicit requirement to understand the purpose and ensure it is both commensurate with the customer and **legitimate** before execution
 - High Risk area



Suspicious Transaction Reports

- To what extent does the AI understand and carry out, their detection and reporting obligations on the suspected proceeds of crime?





Suspicious Transaction Reporting

- P&P for resolution / escalation
 - Need Guidance
 - Timeframe to review internal reports / submit a report to the JFIU
 - Need tipping off reminder in acknowledgement
- Limited Scope of Reviews
 - Period of transaction history attached to the STR
 - Connected accounts
- Quality of internal/external Reports
 - Period of transaction history attached to the STR
 - Basic customer information should be included in the disclosure (e.g. business nature, usual transaction counterparties, etc.)



Wilfully Blind?

- REVIEW the risk
- MONITOR the risk
- MITIGATE the risk
- Requirement for P&P to support these steps

Reminder - consent is only a word –
NOT a risk assessment



Is your STR output effective?

- Should consider, to what extent are the STRs provided by your AI submitted in a timely manner, containing relevant information that allows the JFIU to
 - Understand the basis of the suspicion
 - Conduct a proper analysis
 - Develop operational and strategic analysis





Role of CO/MLRO

- MLRO should play an active role
 - the central reference point for STR
 - involved in the review of MIS etc
 - involved in testing the system
- MLRO should have sufficient experience and exercise appropriate judgement call on suspicious activities identified
- Role of CO
 - Where a compliance function is assigned to other parties (e.g. frontline staff), need compliance review on the work done
 - Need compliance testing, cannot rely completely on internal audit



Recap - MLRO

Paragraph 7.19

An FI should appoint a Money Laundering Reporting Officer (MLRO) as a **central reference point** for reporting suspicious transactions. The FI should have **measures in place to check, on an ongoing basis that it has policies and procedures to ensure compliance** with legal and regulatory requirements and of **testing** such compliance. The type and extent of the measures to be taken in this respect should be appropriate having regard to the risk of ML/TF and the size of the business.



Responsibility of the MLRO

Paragraph 7.21

It is the responsibility of the MLRO to consider all internal disclosures **he receives** in the light of full access to all relevant documentation and other parties. However, the MLRO should not simply be that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the MLRO should play an **active role** in the identification and reporting of suspicious transactions. This **may also involve regular review of exception reports** or large or irregular transaction reports as well as ad hoc reports made by staff.



Law Enforcement Requests

- Expectation - policy and procedures
 - A list / register / centralized record of all law enforcement requests received
 - Handle by appropriate personnel – normal legal / compliance
 - Screening
 - Ensure proper actions both on and offshore
 - Trigger Event! - Appropriate review of accounts subject to court order AND any ML/TF risk the relationship may present



Don't retain law enforcement data

*for longer than necessary to
fulfil the
purpose for
which it
was collected*





Other Observations

- Large cash deposit
 - Need to ascertain whether source of funds and source of wealth are commensurate with customer background
 - Not to record account transfers as cash transactions
- Non-account holder transactions
 - Ensure ID copy is retained on file for transactions of HKD 120,000 or more
- CDD – should not allow customers use personal accounts for business purposes



Stewart McGlynn
Tel. 2878 1095
smcglynn@hkma.gov.hk