INTEGRIUM

# Regulatory Update

24 August 2022

www.integrium-sg.com

# STRENGTHENING AML/CFT PRACTICES FOR EXTERNAL ASSET MANAGERS

24 August 2022

## INTRODUCTION

The Monetary Authority of Singapore ("**MAS**") has published an information paper on "Strengthening AML/CFT Name Screening Practices for External Asset Managers" (the "**Paper**"). The Paper sets out MAS' observations of the thematic inspections done on external asset managers ("**EAMs**"), the good practices observed, and areas where EAMs can improve on.

While the paper is based on EAM inspections and engagements, the insights are relevant to different fund management business models. As a result, all fund management companies ("**FMCs**") should adopt the learning points from the paper when applicable. The results and instances mentioned in the paper are non-exhaustive, and the MAS expects FMCs to continuously improve their AML/CFT frameworks and controls to ensure they are proportionate to the size, nature, and complexity of the company.

The scope of MAS' thematic inspection included:

- Governance;
- Risk Assessment Frameworks;
- Customer Due Diligence ("**CDD**");
- Enhanced CDD; and
- Suspicious Transactions Reporting ("**STR**").

Each of the above areas of inspection is discussed below at further length.

# GOVERNANCE

To successfully reduce money laundering and terrorist financing risks, Board and Senior Management ("**BSM**") should foster a strong AML/CFT culture within the EAMs and actively oversee the formulation and execution of AML/CFT programs throughout the three lines of defence.

## *Areas of weakness observed*

I. Poor risk awareness and failure to set the right tone from the top – This includes EAMs' senior management accepting the onboarding of higher ML/TF risk clients without considering the effectiveness of the enhanced due diligence steps that are implemented. The information acquired and incorporated into the EAMs' evaluation being incorrect or inadequate to support the consumers' declared profiles. This also involves failures and weaknesses not being detected by the top management resulting in red flags not being spotted or effectively followed up on. The institutional process for frequent meetings/forums where discussions and decisions are properly recorded and monthly reports on key ML/TF indicators are presented being inadequate. On top of that, no disciplinary actions taken against key personnel, and representatives not held accountable for the inadequate execution of AML/CFT controls and non-compliance. Additionally, the enterprise-wide risk assessment ("**EWRA**") being incorrect, and the CEO and Chief Operating Officer not being aware of these inaccuracies.

II. Inadequate compliance and/or IA arrangements – This involves BSM not ensuring that its second line of defence is kept up with the expansion and maintained insufficient monitoring of the increased ML/TF risks, compliance resources being inadequate, and no AML/CFT audits conducted by internal audit ("**IA**") or in some cases IA role undertaken by non-independent individual with no relevant audit expertise.

## *MAS expectations*

BSMs are expected to be aware of the regulatory requirements and expectations, set the right ML/TF risk culture and maintain adequate oversight of ML/TF matters through proper monitoring and escalation mechanisms. They must thoroughly evaluate, and question material submitted to them for approval to ensure that it appropriately reflects the EAM's exposure to ML/TF risks. They should ensure that all three lines of defence are aware of their AML/CFT responsibilities, held to account, and equipped with the relevant knowledge to detect ML/TF red flags. They are required to ensure that compliance resources, in terms of skill, experience, and personnel, are proportionate to the EAM's ML/TF risk profile. Lastly, BSMs are to ensure that IA function is independent and adequately resourced with relevant expertise and knowledge of local AML/CFT requirements.

# RISK ASSESSMENT FRAMEWORK

## Enterprise-wide risk assessment

EWRA helps EAMs identify their total exposure to ML/TF risks and establish a holistic approach to managing and mitigating the ML/TF risks that exist across all of their business units, product lines, and delivery channels. It was noted that most EAMs employed a combination of quantitative and qualitative indicators in their EWRA, which were evaluated on a regular basis.

### *Areas of weakness observed*

I. Failure to consider relevant risk factors in the EWRA – This includes failure to take into account important risk variables in the EWRA (e.g. failing to take into consideration risk variables such as the number of higher ML/TF clients and politically exposed individuals ("**PEPs**")), not taking into account the aggregated volume of their customers' transactions which might suggest increased ML/TF, and not taking into account the ML/TF risks connected with the various products or services supplied or the various delivery channels employed such as when the EAM used technology or third parties to execute CDD.

II. Lack of clarity on EWRA methodology – This includes failing to provide enough staff training on its EWRA approach, not specifying the thresholds for quantitative risk factors like “low”, “medium”, or “high”, which results in flawed assessments, and EWRA being treated as checkbox exercise with no fields for staff to provide supporting reasons.

III. Inconsistent rating framework across individual customer risk assessments and EWRAs – This involves EAMs not being consistent with the rating framework and incorrectly adopting a less stringent country risk classification in its EWRA compared to its individual customer risk classification resulting in country exposure at the enterprise-wide level being understated.

IV. Errors in EWRA – This includes "nil" answer to risk variables such as the number of customers residing in countries where corruption or terrorism were prominent but the presence of recent audit report indicating the opposite, and the sum of the risk factor percentages in EWRA not adding up to 100%.

V. No timely review and update of EWRA – This involves an unreasonable amount of time to update their EWRAs, with the longest time taken being four years.

### *MAS expectations*

MAS suggested taking into account all important risk variables, as well as its business strategy, target markets, and delivery methods when assessing ML/TF risks at the enterprise-wide level, ensuring consistency in the use of the risk assessment approach at both the individual customer and enterprise-wide level, providing adequate guidance and conduct proper reviews of EWRAs to ensure accuracy, and review the EWRA on a regular basis at least once every two years or when a material trigger event occurs.

# RISK ASSESSMENT FRAMEWORK

## Customer risk assessment

All EAMs were found to have examined several risk criteria when determining a customer's overall ML/TF risk rating, including, but not limited to, the customer's or beneficial owner's ("**BO**"), place of domicile and nationality, the nature of employment or business, PEP exposure, adverse news, sanctions, the complexity of ownership structure (for corporate customers), and the type of product or service offered. Most EAMs used quantitative methodology and classified clients as having greater ML/TF risks if their aggregate risk score surpassed a particular threshold and/or certain high-risk characteristics were met.

### *Areas of weakness observed*

I. Failure to consider relevant risk factors in identifying higher ML/TF risk customers – This includes EAMs only considering countries that the Financial Action Task Force ("**FATF**") identified to have weak measures to combat ML/TF risks as high risk, not including the countries with corruption and tax evasion risk concerns, and not considering customers with frequent or significant payments received from/sent to unknown or unassociated third parties.

II. Poor execution of customer risk assessment framework – This involves giving customer a medium risk rating and not considering the dual citizenship and country where customer wealth is derived from and failing to consider customers' association with PEPs in some cases.

III. Inadequate CDD applied to PEPs – This includes not subjecting customers to enhanced CDD even where the BOs were plainly PEPs or close associates of PEPs.

IV. Limitation in the design of the customer risk assessment framework – This involves a poorly defined methodology that enables a foreign PEP not to be classified as a high-risk customer.

### *MAS expectations*

I. EAMs should be cognisant of regulatory guidance and ensure that all relevant risk factors are duly incorporated in its customer risk assessment framework.

II. EAMs should consider pertinent and credible information to assess the ML/TF risks posed by customers/BOs, including PEPs, family members, and close associates of PEPs.

III. EAMs should execute the customer risk assessment framework regularly to ensure all higher ML/TF risk customers are appropriately identified and subjected to enhanced CDD measures.

# RISK ASSESSMENT FRAMEWORK

## Customer due diligence – On-boarding of new customers

It was a general observation that most EAMs performed the necessary verification and screening checks to identify the customer and any BOs using onboarding forms and checklists, subscribed to commercial screening databases, and performed internet searches to complement the searches done through their screening databases.

### *Areas of weakness observed*

I. Inadequacies in the identification of customer and their relevant parties – This includes wrongly identifying the party to be the customer and failing to accurately identify the BO and the natural person appointed to act on behalf of the customer.

II. Lack of justification for deferring the completion of CDD measures - This involves not verifying the customer before signing the mandate and EAM postponing the CDD without appropriately managing the ML/TF risks.

III. Inadequacies in the screening process – This includes errors resulting from not having a framework in place for an independent review of screening results, and lack of documentation of screening results.

### *MAS expectations*

MAS suggested EAMs to ensure that its customers and other relevant third parties are correctly recognised. They must ensure that the verification of customers is completed within 30 business days with proper justification as to why deferral was essential. EAMs are to document their screening results properly and ensure that such results are subject to independent reviews.

# RISK ASSESSMENT FRAMEWORK

## Customer due diligence – Transaction monitoring

For EAMs transaction monitoring was performed manually by the compliance function and in some cases EAMs clearly informed the customers that the accounts under EAMs discretionary management will be used solely for investment purposes and this was monitored for adherence on an on-going basis by the EAMs.

### *Areas of weakness observed*

I. Inadequacies in the design of transaction monitoring framework – This includes not establishing any threshold and not tailoring the review in accordance with the customer's risk profile, and not requiring customers to explain the transfer of funds even when amounts were significant and involved third parties.

II. Failure to pick up suspicious transactions across multiple managed accounts belonging to the same BOs – This involves failing to notice and escalate a series of third-party transactions alternating between two accounts handled separately by the same BOs which suspiciously came from an undeclared source of wealth ("**SOW**").

III. Failure to pick up suspicious transactions involving interconnected managed accounts - This involves a group of consumers making several deposits and transactions in a single stock within a few months, and the EAM neglecting to investigate further despite the total sums being out of line with the customers' background, net worth, and income level. EAM failed to identify that customers could be connected to the company they had traded in.

IV. Failure to follow up on anomalies concerning personal transactions in investment management accounts – This involves an anomaly where EAM fails to identify the transfer of funds by customers concerning personal transactions for antique books from brokers that were not in the business of dealing with antique books.

### *MAS expectations*

EAMs should implement a proper transaction monitoring system (including risk-based parameters and thresholds) to discover and report suspicious or anomalous transaction patterns, review transactions holistically across multiple managed accounts belonging to the same BOs or group of interconnected managed accounts, and scrutinise all transactions through the customers' managed accounts involving third parties, those highlighted by custodian banks for possible concerns, and those exhibiting complicated or odd patterns.

# RISK ASSESSMENT FRAMEWORK

## Customer due diligence – Periodic reviews

For most EAMs periodic review was kept to their stipulated review frequency, with higher-risk customers accorded more frequent reviews.

### *Areas of weakness observed*

I. Lack of assessment in retaining customers suspected to be connected with ML/TF – This involves EAMs continuing to retain the customers who are suspected of ML/TF and were alleged to be involved in bribery without any proper justification.

II. Ineffective execution of ongoing measures to detect and manage heightened ML/TF risks – This includes failing to account for any changes in the customer's account, new adverse information, or changes in identifiers (e.g. residential address) resulting in an ineffective execution.

### *MAS expectations*

MAS suggests two takeaways, first, for EAMs to provide proper justification for retaining the customers who are suspected of ML/TF, providing proper documentation and approval by the BSM. Second, EAMs to ensure periodic reviews consider all relevant ML/TF risk areas and regularly assess whether the CDD measures imposed are still commensurate with the customers' updated risk profiles.

# ENHANCED CUSTOMER DUE DILIGENCE

EAMs generally had frameworks in place to perform enhanced CDD measures on customers with ML/TF risks. These measures included seeking senior management approval for business relations, establishing the source of wealth and funds for the customer and its beneficial owners, and conducting enhanced monitoring of business relations.

## *Areas of weakness observed*

I. Failure to promptly identify and conduct enhanced monitoring on higher risk customers – This involves cases such as failure to promptly identify and conduct enhanced CDD on higher-risk customers, a lack of classification of high-risk customers despite awareness of adverse information, and classification of a customer as high risk without further action to subject them to enhanced CDD.

II. Lack of corroboration of customers' SOW and source of funds ("**SOF**") – This includes cases where EAMs failed to corroborate SOW and/or SOF, merely relied on customer representations without obtaining any supporting documents or information, and did not verify that documents substantiated the declared SOW and SOF.

## *MAS expectations*

The MAS stressed the importance of promptly identifying and subjecting customers or beneficial owners posing higher ML/TF risks to enhanced CDD measures and performing adequate independent verification of their SOW and SOF to assess their legitimacy. EAMs should also determine if the measures taken to obtain and confirm the provided information are sufficient and reasonable.

# SUSPICIOUS TRANSACTION REPORTING

EAMs must file STR with the Suspicious Transaction Reporting Office if they suspect a transaction is connected to ML/TF within 15 working days of the case being flagged as suspicious.

## *Areas of weakness observed*

I. Lack of awareness to file STRs on customers with adverse information or conduct that suggested linkage to financial crime – This involves not filing STRs despite having knowledge of customers/beneficial owners of corporate customers participating in tax amnesty programmes ("**TAPs**"), the customer being involved in ongoing legal proceedings for a money laundering case, multiple large deposits by a group of interconnected customers into their respective managed accounts that are not consistent with the EAM's knowledge of their SOW and SOF, and a custodian bank raising concerns about the legitimacy of a customer's funds to the EAM.

## *MAS expectations*

The MAS emphasises on the filing of STRs on customers if EAMs know or have reasonable grounds to suspect that the customer's property could be connected to ML/TF.

## CONCLUSION

Deficiencies in AML/CFT practices were observed in a few EAMs during inspections and engagement. EAMs should be aware of their inherent vulnerability to ML/TF risks, establish appropriate risk cultures and controls, equip staff with the necessary knowledge and resources to effectively implement AML/CFT frameworks, continuously improve AML/CFT frameworks to be proportionate to the scale, nature, and complexity of their business, and be aware of regulatory guidance and expectations.

## Contacts

**Mark Jacobsen**
Founder
Integrium

**E** mark@integrium-sg.com

**Dewansh Raheja**
Manager
Integrium

**E** dewansh.raheja@integrium-sg.com

**Integrium Pte. Ltd.**
63 Chulia Street
#15-01
Singapore 049514
**www.integrium-sg.com**