NOTE ON MAS' INFORMATION PAPER ON STRENGTHENING AML/CFT PRACTICES FOR EXTERNAL ASSET MANAGERS

Posted on November 17, 2022

Category: CNPupdates

Published: 17 November 2022

Authors: Bill Jamieson

This note summarises MAS' information paper (dated August 2022) on strengthening anti-money laundering and countering the financing of terrorism ("AML/CFT") framework and controls for external asset managers ("EAMs"). Although the information paper sets out the best practices and supervisory expectations for EAMs, MAS has clarified that the takeaways in the paper are also applicable to other fund management companies, where relevant. The list of issues (in a thematic form) that have been observed but are discouraged by MAS are set out below:

1. Governance Issues – Board and Senior Management ("BSM")

(a) Poor risk awareness and failure to set the right tone from the top

- **Lack of caution in exercising relevant approvals**: Senior management of some EAMs approved the onboarding of higher money laundering and terrorism financing ("ML/TF") risk customers without considering the adequacy of enhanced due diligence measures. Specifically, the BSM failed to pick up inaccurate or insufficient data/information that supported the customers' declared profiles.
- **Governance failures**: An EAM had multiple governance failures. Specifically, the EAM had no formal mechanisms (e.g. regular meetings/forums where discussions and decisions were properly recorded) to ensure accountability and allow BSM to keep track and stay updated on key ML/TF issues. The EAM also did not have key performance indicators, and key staff and representatives were not held accountable for their poor execution of AML/CFT controls and non-adherence with regulatory requirements as well as internal policies and procedures. There were also repeat findings from a past MAS inspection, which indicated that remediation measures were ineffective.
- **Failure to pick up errors**: Errors in the enterprise-wide risk assessment ("EWRA") were not picked up by BSM – these errors affected the accuracy of the EAM's ML/TF risk assessment at the enterprise-wide level.

(b) Inadequate compliance and/or Internal Audit ("IA") arrangements

- **Lack of Independent IA function**: An EAM allowed a non-independent person who had no relevant audit experience and knowledge of local AML/CFT requirements to perform the IA function.
- **Inadequate compliance with growth of business**: An EAM did not ensure its second line of defence kept pace with the substantial growth of business and failed to maintain proper oversight of the heightened ML/TF risks posed. Specifically, compliance resources were grossly insufficient and there were no AML/CFT audits by IA during the growth period.

- **Failure to assess AML/CFT policies**: A handful of EAMs also failed to conduct any internal audits to assess the effectiveness of their AML/CFT policies, procedures and controls.

2. Risk Assessment Frameworks

2.1 EWRA

(a) Failure to consider relevant risk factors in the EWRA

- **Failure to consider customer profiles**: In conducting risk assessments, an EAM failed to consider the ML/TF risk profile of its customers. Another EAM who managed both segregated mandates and funds did not consider the ML/TF risk profile of its funds' customers. A number of EAMs did not consider ML/TF risks associated with the target customer markets and segments.
- **Failure to consider customer transactions**: Some EAMs did not consider the aggregated volumes and sizes of their customers' transactions and fund transfers which could be indicative of heightened ML/TF risks if the transactions involved third parties and/or high-risk countries. This included customers for which the EAMs do not have full control over the management of the customers' assets (e.g. customers could direct payments to third parties).
- **Failure to consider personal transactions**: An EAM allowed personal transactions (e.g. purchase of high value goods) to be undertaken in customers' investment management accounts without assessing whether such transactions heightens the ML/TF risks at the enterprise-wide level.
- **Failure to consider products/services and delivery channels**: Some EAMs did not consider the types of products/services that were offered and their associated ML/TF risks. Some EAMS did not consider the ML/TF risks arising from different delivery channels (i.e. extent to which the EAM leveraged on technology or relied on third parties to perform customer due diligence measures).

(b) Lack of clarity on EWRA methodology

- **Unclear EWRA methodology**: Some EAMs did not provide guidance to staff on how the different EWRA risk and control factors should be rated. For example, an EAM did not provide guidance nor did it specify the thresholds for the assignment of different ratings (i.e. thresholds for rating quantitative risk factors "Low", "Medium" or "High"). The methodology to determine the overall EWRA rating was also not specified.
- **Unsubstantiated EWRA**: The EWRA should not be a check-box exercise with only 'Yes/No' inputs and no supporting justifications and assessments.

(c) Inconsistent rating framework for individual customer risk assessments versus EWRA

- An EAM lacked a consistent risk framework for both individual customer and enterprise-wide level. Specifically, the EAM adopted a less stringent country risk classification for its EWRA compared to its individual customer risk assessment. This resulted in the understatement of its ML/TF risks associated with its country exposure at the enterprise-wide level.

(d) Errors in EWRA

- **Errors in EWRA**: An EAM had errors in its EWRA, thereby affecting the accuracy of its ML/TF risk assessment at the enterprise-wide level. Specifically, the EAM provided nil responses to certain risk factors despite the response being inconsistent with its most recent internal audit report.
- **Errors in EWRA's methodology**: An EAM's EWRA methodology was mathematically flawed and the EAM could not provide logical explanations for its computations – specifically, the sum of all the risk factors did not add up to 100%.

(e) No timely review and update of EWRA

- Some EAMs took more than two years to update their EWRAs. Reviews should be done at least once every two years or when material trigger events/developments occur, whichever is

2.2 Customer risk assessment

(a) Failure to consider relevant risk factors in identifying higher ML/TF risk customers

- **Failure to consider higher risk countries**: To identify high risk countries, some EAMs only considered those highlighted by Financial Action Task Force ("FATF") as having weaker ML/TF precautions. EAMs ought to also consider other country-specific assessments by FATF (e.g. mutual evaluation reports) and/or include countries with corruption and tax evasion risk concerns identified by other credible bodies (e.g. Transparency International, the Organisation for Economic Co-operation and Development).
- **Failure to consider higher tax risks**: In assessing tax risks, some EAMs failed to consider customers' participation in tax amnesty programmes. Another EAM considered the "existence of specific transactions" as one of the tax risk indicators without defining what these "specific transactions" were.
- **Failure to consider frequency of payments received from/sent to third parties**: Some EAMs did not consider customers with frequent or significant payments received from/sent to unknown or unassociated third parties as posing higher ML/TF risks.

(b) Poor execution of customer risk assessment framework

- **Inaccurate categorisation of Politically Exposed Persons ("PEPs")**: Some EAMs failed to consider some customers as having political exposure even though they were aware of the

customers' association with PEPs. Additionally, where a customer is a citizen of two countries, one of which is a country that FATF called for counter measures, EAMs should consider the higher risk posed by the customer.

(c) Inadequate CDD applied to PEPs

- Despite having customers where the beneficial owners ("BOs") were considered PEPs or close associates of PEPs, an EAM did not subject these customers to enhanced CDD.

(d) Limitation in the design of the customer risk assessment framework

- An EAM's risk rating methodology allowed a foreign PEP not to be classified as a "High" risk customer (where enhanced CDD would apply) when the cumulative score was less than "X", which was against the regulatory requirement for all foreign PEPs to be subjected to enhanced CDD.

3. Customer Due Diligence

3.1 Onboarding of new customers

(a) Inadequacies in the identification of customer and their relevant parties

- **Failure to identify customers**: An EAM appointed by trustees to be the investment manager for some investment-linked policies ("ILPs") funded by trust assets misidentified the insurance company as customer instead of the trustees. The trustees should have been identified as customer instead of the insurance company that issued the ILPs.
- **Failure to identify customers**: Some EAMs did not inquire on the BOs of customers with trust structures where the trustees were financial institutions. Some EAMs also failed to identify, screen, and verify the natural persons (including their due authority) who were appointed to act on behalf of the customer.

(b) Lack of justification for deferring the completion of CDD measures

- Some EAMs failed to verify the identities of customers and their relevant parties before establishing business relations. In other words, the EAMs failed to verify the identification documents of a customer before signing the asset management mandate with the customer. The EAMs also failed to justify why the deferment of the verification process was necessary. Even with proper justification, EAMs are reminded that the completion of the outstanding verification should not exceed 30 business days after the establishment of business relations.

(c) Inadequacies in the screening process

- **Delays in screening**: Some EAMs were not familiar with the screening requirements for their customers and the relevant parties. As such, they did not screen them when, or as soon as reasonably practicable after, they had established business relations with the customers.
- **Lack of controls in the screening process**: Some EAMs had no adequate controls over the review of screening results. For example, in one case, the staff responsible for screening and reviewing the screening results during onboarding was able to dismiss any screening hits singly without any justifications or independent review by another party.
- **Lack of documentation on screening results**: Some EAMs did not document their assessment of the screening results for screening hits. Additionally, the reasons for the EAMs' decision to onboard or continue business relation with the customer where there was a positive screening hit were also not properly documented.

3.2 Transaction Monitoring

(a) Inadequacies in the design of transaction monitoring framework

- **Inadequate monitoring**: Most EAMs did not monitor transactions across multiple managed accounts belonging to the same customer(s)/BO(s). Additionally, some EAMs' transaction monitoring was limited to reconciling trading records against custodian bank records.
- **Failure to query**: Most EAMs did not have any requirements to query their customers on the transfer of funds into and out of the managed accounts on an ongoing basis, even where the amount was significant and/or involved third parties.
- **Inadequacies in the design of transaction monitoring framework**: Some EAMs' transaction monitoring framework did not include risk-based parameters and thresholds and/or tailor the frequency of review to different customer risk profiles to promptly detect and report suspicious, complex, unusually large, inconsistent or unusual patterns of transactions in their customers' accounts on an ongoing basis.

(b) Failure to pick up suspicious transactions across multiple managed accounts belonging to the same BOs

- An EAM failed to detect/review a series of third-party transfers alternating between two separate managed accounts that belonged to the same BOs over an extended period of time. Although both accounts were for investment management purposes, there were no investments made in one of the accounts. The source of the transfers was also not in line with the customers/BOs' declared source of wealth ("**SOW**") and source of funds ("**SOF**").

(c) Failure to pick up suspicious transactions involving interconnected managed accounts

- An EAM failed to investigate and escalate suspicious transactions. Specifically, the suspicious transaction was the making of multiple deposits and trades in a single stock within a period of a

few months by a group of customers.

(d) Failure to follow up on anomalies concerning personal transactions

- An EAM failed to enquire further on anomalies noted and escalate the anomalies internally. Specifically, the anomaly involved the use of funds in an account (independently managed by the EAM) to purchase antique books from brokers that were not in the business of dealing in antique books.

3.3 Periodic Review

(a) Lack of assessment in retaining customers suspected to be connected with ML/TF

- Despite reasonable grounds for suspicion (i.e. allegations of bribery) that an existing customer is connected with ML/TF, an EAM did not substantiate and document the reasons for retaining the customer.

(b) Ineffective execution of ongoing measures to detect and manage heightened ML/TF risks

- **Ineffective execution of customer reviews**: An EAM's customer reviews did not cover changes to the customers' circumstances (e.g. financial or professional status), adverse information flagged from screening checks, and changes in the nature, size and frequency of transactions noted in the customers' account.
- **Ineffective execution of validity checks**: An EAM's annual validity checks on customers only reviewed (i) identification documents of individual customers, and (ii) register of members and directors of corporate customers. The EAM failed to review documents and information (e.g. residential address) used to identify customers and their relevant parties.
- **Ineffective execution of approval process for reviews**: Although an EAM required senior management's sign-off for "High" risk customers reviews, there were instances where reviews of "High" risk customers were either omitted, submitted late without reasons or not signed off by senior management.

4. Enhanced CDD

(a) Failure to promptly identify and conduct enhanced monitoring on higher risk customers

- An EAM failed to promptly classify a customer as "High risk" when adverse information concerning the customer surfaced. The same adverse information was subsequently made known to the compliance team later. While the customer's risk rating was elevated then, the customer was further omitted from enhanced monitoring due to the compliance department's oversight for a period of time.

(b) Lack of corroboration of customers' SOW and SOF

- **Lack of supporting documents and use of arbitrary assumptions**: A customer had attributed his SOW and SOF to investments. However, the EAM failed to obtain information about the nature and composition of the customer's investments. Instead, the EAM made assumptions concerning the customer's savings and the investments' annual rate of return without adequate basis.
- **Failure to follow up on customers with new risk profiles**: Despite the raise of a customer's risk profile to "High", supporting documents to substantiate the BOs' SOW and SOF were not obtained. The EAM had instead made certain assumptions concerning the business' net profit margin. Additionally, discrepancy between the declared duration of the BOs' business and the period reflected in public documents was not detected and followed up on.
- **Lack of independent verification of customers' SOW and SOF (inheritance)**: A BO's SOW and SOF were from the BO's deceased spouse. However, the EAM did not obtain any documentary evidence to corroborate the inheritance and subsequent documentation obtained by the EAM following MAS' queries could only verify a fraction of the amount declared.
- **Lack of independent verification of customers' SOW and SOF (business)**: An EAM failed to corroborate the income of a "high" risk customer against independent documentary evidence or public information sources. Although an audit firm was appointed to perform agreed-upon procedures ("AUP") to establish the customer's SOW from his other businesses, the customer was onboarded prior to the submission of the draft AUP report, and anomalies in the AUP report were not questioned or followed up on.

5. Suspicious Transactions Reporting ("STR")

- **Lack of awareness to file STRs on customers with adverse information or conduct that suggested linkage to financial crimes:** Some EAMs failed to file an STR on a customer despite having reasonable grounds to suspect that any property of the customer could be connected to ML/TF. Specifically, no STRs were filed despite the EAMs having knowledge of the following:
  - Customers/BOs of corporate customers participation in tax amnesty programmes.
  - Customer's involvement in ongoing legal proceedings for a money laundering case.
  - Multiple large deposits by a group of interconnected customers into their respective managed accounts, which were not consistent with the EAM's knowledge of their SOW and SOF.
  - Concerns raised about the legitimacy of the customer's funds to the EAM by custodian banks servicing the same customer.