香港海關
Customs and Excise Department

MSSB/MIS_03/2023
22 November 2023

Circular

Circular to Money Service Operators

Anti-Money Laundering / Counter-Terrorist Financing ("AML/CFT")

Supervisory Findings of Customer Due Diligence ("CDD") Related Issues

This circular highlights the deficiencies or inadequacies identified by the Customs and Excise Department ("C&ED") from compliance inspections of licensees' AML/CFT policies, procedures and controls (collectively referred to as "AML/CFT systems"). We also provide expected regulatory standards and non-exhaustive examples of good practices to assist money service operators ("MSOs") in reviewing the adequacy of their AML/CFT systems.

Compliance inspections took an in-depth look at, among other measures, the implementation of risk-based CDD measures of selected licensees where some critical deficiencies and non-compliance were identified. The critical areas to which MSOs should pay priority attention are as follows:

1. Inadequate consideration of pertinent money laundering and terrorist financing ("ML/TF") risk factors when conducting customer risk assessments, as well as inadequate follow-up on the assessment results. MSOs must address the assessed ML/TF risks by reviewing whether the overall ML/TF risk level of any of their existing customers should be elevated when any risk factor with which they are associated is assessed to pose a higher risk than before.

2. Failure to identify and take reasonable measure to verify the beneficial owner in relation to the customer, and thereby undermining the effectiveness of an MSO's politically exposed persons ("PEPs") and sanctions screening mechanism.

3. Inadequate measures to verify authority of the person purporting to act on behalf of the customer ("PPTA") as required by the Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("AMLO")[1] and the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For MSOs) ("AML Guideline").[2]

To facilitate compliance, the above-mentioned inspection findings as well as expected regulatory standards and examples of good practices[3] are set out in the **Appendix**. MSOs should review their AML/CFT systems in light of this circular and take immediate actions to rectify any deficiencies and non-compliance.

---

[1] Sections 2 and 3 of Schedule 2 to the AMLO.
[2] Paragraphs 4.5.1 to 4.5.4 of the AML Guideline.
[3] These examples are not meant to be exhaustive and should not be regarded as the only ways of meeting the regulatory requirements.

MSOs should consider and assess whether any of these practises should be appropriately adopted in their own AML/CFT system, in a bid to not only meet the legal and regulatory obligations under the AMLO and the AML Guideline, but also to implement effective measures to further mitigate their ML/TF risks.

The C&ED will continue to monitor AML/CFT compliance and will not hesitate to take regulatory action, including enforcement and disciplinary sanctions, where appropriate, against MSOs for breach of the AML/CFT requirements. As part of the ongoing effort to improve AML/CFT compliance, particularly in areas where deficiencies and inadequacies are detected, the C&ED will continue to provide regulatory guidance to assist MSOs in enhancing their AML/CFT systems.

Should you have any queries regarding the contents of this circular, please contact us at 3742 7787.

Money Service Supervision Bureau

Customs and Excise Department

End

Appendix –
Deficiencies and inadequacies in meeting the expected regulatory standards

(1) Customer risk assessment ("CRA")

Deficiencies or inadequacies
➢ Some MSOs failed to follow up on inconsistent information provided by customers (e.g. individual customers declared the purpose of the business relationships as personal remittance but provided company addresses as address proofs and claimed payment for goods as the transaction purpose) to ensure the conduct of adequate CDD. ➢ Some MSOs failed to provide sufficient guidance to their management and frontline staff on how to determine a customer's overall ML/TF risk level based on a range of pre-defined risk factors. This resulted in inconsistent ML/TF risk levels being assigned to customers with similar risk factors. ➢ Some MSOs did not maintain sufficient documentation to show how individual customers' ML/TF risk levels were derived. This undermined the effectiveness of any subsequent compliance reviews to ensure proper adherence to the MSOs' customer risk assessment policies and methodologies.

An MSO should properly identify and categorise ML/TF risks at the customer level by considering all relevant risk factors, differentiate customers presenting a higher ML/TF risk and apply enhanced measures to manage and mitigate the risk.[4]

An MSO should provide sufficient guidance to staff and put in place adequate procedural safeguards to ensure that they conduct CRA in compliance with the regulatory requirements and the MSO's policies. MSO should, inter alia, ensure that their staff follow up on inconsistent information provided by customers to establish accurate customer profiles and require their staff to keep proper records of CRAs together with relevant documents to demonstrate how they assess individual customers' ML/TF risk levels.[5]

Where an MSO ascertains that a customer has misled the MSO about the purpose and intended nature of the business relationship, or identifies that the transactions carried out for the customer are not consistent with the MSO's knowledge of the customer and the customer's risk profile, the MSO should take prompt action (e.g. examining the background and purposes of the transactions; making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion.[6] Where the MSO cannot obtain a satisfactory explanation of the transaction, it may conclude that there are grounds for suspicion. In any event where there is any suspicion identified during transaction monitoring, a suspicious transaction report should be made to the Joint Financial Intelligence Unit.[7]

---

[4] Paragraphs 2.13 to 2.14 and 4.9.5 of the AML Guideline.
[5] Paragraph 2.16 of the AML Guideline.
[6] Section 5(1)(b) & (c) of Schedule 2 to the AMLO; Paragraphs 4.6.1 and 5.10 of the AML Guideline.
[7] Paragraph 5.12 of the AML Guideline.

(2) Identification and verification of a beneficial owner

Deficiencies or inadequacies
➢ In the case of corporate customers, some MSOs failed to obtain any reliable, independent source documents, such as certificates of incorporation or certificates of incumbency, to verify the identities of a corporate customer and its beneficial owners. ➢ Some MSOs failed to identify all beneficial owners (e.g. individuals who ultimately own or control more than a 25% interest) of a corporate customer and verify their identities. ➢ MSOs carried out screening of customers against a commercially available database to identify PEPs and individuals or entities subject to targeted financial sanctions. However, the scope of screening did not extend to the beneficial owners of the customers.

It is a requirement under the AMLO that an MSO must identify customers and verify their identities by using documents, data or information from reliable and independent sources, as well as identify and take reasonable measures to verify the identities of beneficial owners in relation to the customers. Beneficial owners in relation to a corporation include: (a) all individuals who own or control, directly or indirectly, more than 25% of the voting rights or share capital of the corporation; (b) any individuals who exercise ultimate control over the management of the corporation; and (c) any persons on whose behalf the customer is acting.[8]

In determining what constitutes reasonable measures to verify the identity of a beneficial owner of a customer, an MSO should give due regard to the ML/TF risks posed by the customer and the business relationship. Therefore, depending on the associated risks, MSOs should corroborate information collected from the customer with publicly available information for companies' ownership and control structure (e.g. ownership chart) and shareholding information (e.g. annual return, significant controllers register).[9] The objective is to follow the chain of ownerships to the beneficial owners of the customer.

An MSO must establish and maintain effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP. The name screening procedures for the identification of PEPs must cover not only the customer, but also any beneficial owners of the customer.[10]

In addition, to avoid establishing business relationship with or providing any financial services to any terrorist suspects and possible sanctioned parties, irrespective of the risk profile attributed to the customer, an MSO is required to screen its customers and any beneficial owners of the customers, as well as all relevant parties in remittance transactions, against sanctions and designated persons lists.[11]

---

8 Sections 1(1) and 2 of Schedule 2 to the AMLO.
9 Paragraph 4.4.3 of the AML Guideline.
10 Section 19(1) of Schedule 2 to the AMLO.
11 Paragraph 6.16 of the AML Guideline.

(3) Identification and verification of PPTA

Deficiencies or inadequacies
➢ MSOs' procedural failure to obtain authorization documentations (e.g. board resolution or similar written authorization). ➢ Some MSOs failed to identify the corporate customer and treated a PPTA as the customer.

According to the AML Guideline, an MSO should implement clear policies and procedures for determining who is considered to be a PPTA. Whether the person is considered to be PPTA should be determined based on the nature of that person's roles and the activities which the person is authorised to conduct, as well as the ML/TF risks associated with these roles and activities.[12]

An MSO should adopt a framework of procedures in assessing who would ordinarily be considered a PPTA for each customer segment, with the approach and rationale consistent across the MSO's departments. As a general proposition, each legal person customer should have at least one PPTA (i.e. the person acting on behalf of a customer to establish the business relationship with the MSO as mentioned above).

As indicated in paragraph 4.5.3 of the AML Guideline, the MSO is required to identify the PPTA by obtaining at least the following identification information:

In the case of a natural person PPTA, (a) full name; (b) date of birth; (c) nationality; and (d) unique identification number and document type.

In the case of a legal person PPTA, (a) full name; (b) date of incorporation, establishment or registration; (c) place of incorporation, establishment or registration (including address of registered office); (d) unique identification number and document type; and (e) principal place of business (if different from the address of registered office).

Regarding the authorization to evidence the PPTA's authority, paragraph 4.5.4 of the AML Guideline provides that "*an MSO should verify the authority of each PPTA by appropriate documentary evidence (e.g. board resolution or similar written authorization)*."

[12] Paragraph 4.5.1 of the AML Guideline.