香港海關
Customs and Excise Department

MSSB/MIS_02/2023

Circular

31 May 2023

Circular to Money Service Operators

Anti-Money Laundering / Counter-Terrorist Financing

Consultation Conclusions on the Revised Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (Revised AML/CFT Guideline)

Following the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022 ("the AMLO") published in the Gazette on 16 December 2022, the Customs and Excise Department ("C&ED") conducted an industry consultation between 20 April 2023 and 11 May 2023 on the proposed amendments to the Guideline on Anti-Money Laundering and Counter- Financing of Terrorism (For Money Service Operators) ("AML/CFT Guideline").

Throughout the revision of the AML/CFT Guideline, the C&ED collaborated with stakeholders, including other regulators and the Money Service Operators Association (MSOA) for setting common and principles-based standards reflecting the amendments in the AMLO, as well as taking into account the latest international standards set by the Financial Action Task Force (FATF). To prepare for the implementation of the amended statutory requirements from 1 June 2023, Money Service Operators ("MSOs") should read in conjunction with this circular and the revised AML/CFT Guideline published in the Gazette on 25 May 2023.

By the end of the consultation, the C&ED received a number of comments and requests for clarification on the amendments in the AML/CFT Guideline from sector members. This circular aims to summarise the key comments received and the C&ED's responses with a view to providing supplementary guidance to the MSO sector for implementing the AML/CFT Guideline.

Digital identification system

Respondents sought clarification on the definition of "a digital identification system that is recognised by the Commissioner of Customs and Excise ("CCE")" and whether technology solutions being used by MSOs for remote customer on-boarding would be recognised digital identification systems.

At present, the CCE and other relevant authorities ("RAs") have agreed that "iAM Smart", a digital identification system developed and operated by the Hong Kong Government, meets relevant FATF requirements and is recognised by RAs under section 2(1)(a)(iiia) of Schedule 2 to the AMLO. "iAM Smart" can be used as an alternative to the physical identification document for meeting the customer identification and verification requirements in the context of remote on-boarding (i.e. during non-face-to-face situations). However, "iAM Smart" by

itself cannot generally help MSOs meet the broader Customer Due Diligence ("CDD") requirements that go beyond customer identification and verification. When designing their remote on-boarding models, MSOs should have regard to the latest features of "iAM Smart" to establish their own CDD or customer on-boarding policies and procedures that are appropriate and proportionate. This may necessitate the collection of additional documents or other information where it is considered necessary for the purpose of CDD, ongoing monitoring or other compliance and risk management.

On selection of technology solutions for remote customer on-boarding, the Hong Kong Government has not set any assurance framework or standard for assessing digital identification systems operated and developed by private sector companies, nor has indicated that it intends to assure, audit or certify such digital identification systems at this stage. Therefore, MSOs should not regard these technology solutions as digital identification systems for the purpose of complying with section 2(1)(a) of Schedule 2 to the AMLO. With the development of technology, it is foreseeable that there will be other systems developed and operated by governments in other jurisdictions which can provide similar functions in the future. The C&ED will keep abreast of the development and issue advisory circular to provide guidance to MSOs in due course.

Beneficial ownership of a trust

Regarding the amended definition of "beneficial owner" in the AMLO in relation to trusts or other similar legal arrangements, respondents have expressed their concerns, especially on the extra efforts needed to be put in identifying and verifying the identity of the trust beneficiaries following the removal of the 25% threshold for trust beneficiaries.

Further to the amendments on Chapter 4 of the revised AML/CFT Guideline, the C&ED has provided supplementary guidance on verifying the identities of beneficiaries in paragraph 4.4.3 of the revised AML/CFT Guideline. An MSO should consider and give due regard to the money laundering and terrorist financing ("ML/TF") risks posed by the customer and the business relationship when determining reasonable measures to verify the identity of a beneficial owner of a customer. MSOs may consider whether it is appropriate to make use of the records of a beneficial owner available in the public domain, request its customer to provide documents or information in relation to the beneficial owner's identity obtained from a reliable and independent source, or corroborate the customer's undertaking or declaration with publicly available information, mainly depending on the ML/TF risk levels of their customers. In exceptionally low ML/TF risk situation (e.g. charitable trust), it may be reasonable for the MSO to confirm the beneficial owner's identity based on the information provided by the customer (including trustee(s) whose identities have been verified). This could include information provided by the customer as to the beneficial owner's identity, and confirmation that they are known to the trustee(s).

In some jurisdictions, corporations are required to maintain registers of their beneficial owners

(e.g. the significant controllers register maintained in accordance with the Companies Ordinance of Hong Kong (Cap. 622)). An MSO may refer to such registers to assist in identifying the beneficial owners of its customers. Where a register of the beneficial owners is not made publicly available, the MSO may obtain the record, including undertaking or declaration directly from its customers (including the trustee of a trust) on the identification information in relation to the beneficial ownership.

Virtual assets (VAs) and virtual asset service providers (VASPs)

To implement the FATF Standards on VAs and VASPs, a licensing regime to be managed by the Securities and Futures Commission ("SFC") is introduced in the AMLO to impose statutory AML/CFT obligations on VAs trading activities and custodian services. The C&ED has reiterated that MSOs are not exempted from the VASP licensing regime and therefore should enquire the SFC if MSOs intend to engage in such businesses.

It is worth noting that the AMLO does not prohibit MSOs from carrying out virtual asset transfers on behalf of customers, provided that the requirements set out in the newly enacted section 13A (i.e. Special requirements for virtual asset transfer) and section 20(3A) (i.e. Record-keeping requirements for occasional transaction not less than $8,000) of Schedule 2 to the AMLO are met.

Customer Due Diligence Requirements

Respondents sought clarification on changes of CDD requirements in the amended AMLO. While the CDD threshold for money changing, wire transfer and remittance in sections (3) and (13) of Schedule 2 to the AMLO remain unchanged, the definition of "occasional transaction" in section (3) of Schedule 2 to the AMLO is revised with the inclusion of "a virtual asset transfer involving virtual assets that amount to no less than $8,000" for carrying out CDD measures in relation to a customer before the transaction takes place.

In addition, MSOs are reminded that there is no one-size-fits-all methodology for conducting CDD as customers may have different characteristics, even when they are from the same business sector. MSOs should establish their own internal risk management mechanism to apply different level of CDD measures based on their risk levels. For concerned issues such as proliferation financing (PF) and other high risk situations, enhanced CDD efforts may be needed for additional safeguards.

AML/CFT Systems in relation to suspicious transaction reporting

For the addition of illustrative red flag indicators in paragraph 7.10 on top of the "SAFE" approach on identifying suspicious transactions promoted by the Joint Financial Intelligence Unit in paragraph 7.11 of the AML/CFT Guideline, this amendment aims to provide a more comprehensive categorization of transactions with examples to assist MSOs to identify potential suspicious transactions. MSOs are advised that the list of red flag indicators is non-exhaustive and is for reference only. MSOs may refer to Chapter 7 and further beef up their

own ongoing monitoring system and internal reporting mechanism which are commensurate with the assessed risks of ML/TF/PF.

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