香港海關
Customs and Excise Department

MSSB/MIS_01/2026
20 January 2026

Circular

Circular to Money Service Operators
Anti-Money Laundering/Counter-Terrorist Financing

Guidance on combating Money Laundering
Associated with Trade-based activities

The Customs and Excise Department ("C&ED") would like to draw Money Service Operators' ("MSOs") attention to the recent trade-based money laundering ("TBML") typologies that involve the use of falsified trade documents, such as fake contracts and invoices, to create bogus transaction records and disguise illicit money as legitimate trade income.

TBML is the process of disguising the proceeds of crime and moving value through the use of trade activities in an attempt to legitimise their illegal origins or finance criminal activities. The C&ED notes with concern that the syndicated TBML activities may pose heightened money laundering and terrorist financing ("ML/TF") threats to the sector. Cross-boundary remittance service offered by MSOs could be exploited as one of the conduits for transfer of the trade-based crime proceeds. In particular, domestic and foreign criminal activities would attempt to use shell companies and fabricated document in order to obscure the identity of the beneficial owner or the source of illicit funds.

In this connection, the risk indicators designed by the Financial Action Task Force ("FATF") are provided to enhance the ability of MSOs to identify suspicious activities associated with the TBML. The relevant FATF website: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Risk-Indicators.pdf

Furthermore, MSOs are reminded to establish adequate and effective anti-money laundering and counter-financing of terrorism ("AML/CFT") controls and continually make enhancement in some areas in order to respond to the evolving and increasingly sophisticated ML/TF methods used by criminal syndicates:

1. Understanding of ML/TF risks

   MSOs' customer risk assessment frameworks should be capable of identifying customers with higher ML/TF risks. In addition, MSOs should ensure that they adequately understand and assess the reasonableness of customer characteristics and/or material changes in customer profiles, and then apply effective additional controls proportionate to their ML/TF risks. Particular attention should also be given to flagging and escalating cases to MSOs' senior management where multiple risk indicators are present on the customers. These efforts need to be supported by adequate training and guidance to staff to facilitate sufficient ML/TF risk awareness in both the first and second lines of defence.

2. Customer due diligence ("CDD")

Besides establishing CDD policies and procedures which meet the statutory and regulatory requirements under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Chapter 615 ("AMLO") and the Guideline on AML/CFT (For MSOs), MSOs should ensure the implementation of their CDD measures are effective and proportionate to the ML/TF risks associated with customers. MSOs should apply Enhanced Due Diligence ("EDD") requirements to customers with high ML/TF risks. The implementation of either CDD or EDD needs to be supported by adequate understanding and assessment of the customers' business and risk profiles and business relationship. MSOs should also consider obtaining information on the Source of Funds ("SoF") and Source of Wealth ("SoW") of the customers for having a better understanding on their profiles.

Moreover, MSOs should pay attention to the much higher ML and TF risks posed for customers who are newly established legal entities without significant assets, employees and/or active business operations. MSOs should proactively consider to apply anti-fraud procedures for scrutinizing information obtained from customers in order to verify the genuineness of the transaction and assess the likelihood of shell companies involved as an originator or a recipient in the concerned transaction. MSO should also periodically review the obtained documents, data and information relating to the customers to ensure that they are up-to-date and relevant.

3. Transaction monitoring ("TM")

Ongoing monitoring is an essential component of effective AML/CFT Systems. The TM systems of MSOs should be able to effectively identify and generate alerts for unusual or suspicious transactions. MSOs should ensure appropriate steps are taken (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, instead of closing generated TM alerts without sufficient justification and analysis. MSOs should also adequately assess the reasonableness of transactions taking into account the customer risk profiles, SoF / SoW and historical transactions.

4. Filing Suspicious Transaction Reports ("STR")

The C&ED reiterates that MSOs are required to report an STR where they suspect that a transaction is associated with proceeds of crime or terrorist property, together with any matter on which the knowledge or suspicion is based. Specifically, when an MSO holds information concerning both the originator and the recipient of funds, the MSO should take into account all of this information in determining whether an STR has to be filed. The reporting obligations require a person to report suspicions of ML/TF irrespective of the amount involved. The obligations also apply whether or not a transaction was actually conducted and cover attempted transactions.

MSOs should review their existing AML/CFT controls through a gap analysis, and give consideration to optimising their AML/CFT controls based on the areas for enhancement outlined above with a view to mitigating the risks associated with TBML and other evolving and increasingly sophisticated methods used by criminal syndicates.

Should you have any queries regarding the contents of this circular, please contact us at 3742 7742.

Money Service Supervision Bureau

Customs and Excise Department

End