香港海關
Customs and Excise Department

MSSB/MIS_01/2024
17 September 2024

Circular

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

Money Laundering and Terrorist Financing Risks Associated with Third Party Payments

The Customs and Excise Department ("C&ED") would like to draw Money Service Operators' ("MSOs") attention to the recent press briefing held by the Ministry of Public Security of the Mainland[1], which reported on the effectiveness of measures taken to combat serious crimes derived from Macao's "money exchange gangs"[2]. The briefing highlights joint efforts of the Ministry of Public Security and the Public Security Police Force of Macao against cross-boundary money exchange syndicates which operate several criminal networks involved in illegal activities related to money laundering ("ML") and underground money exchange with parallel trading of Renminbi and other currencies.

The C&ED notes with concern that the syndicated ML activities in neighbouring regions pose heightened threats to the MSO sector given the geographic proximity and closely connected financial activities among the Mainland, Hong Kong and Macao. Cross-boundary remittance service offered by MSOs, particularly inward remittance initiated by transient customers, could be exploited as a conduit for transfer of crime proceeds. In addition, the vulnerabilities of some MSOs are exacerbated by their **acceptance of payment from third parties**[3], as criminals would attempt to use third party payments for transactions in order to obscure the identity of the beneficial owner or the source of illicit funds.

In particular, an MSO should exercise care if there is suspicion that a customer may be effecting a transaction on behalf of a third party. These transactions may be associated with one or more red flags which should arouse reasonable suspicion in MSOs. If MSOs fail to take reasonable steps to detect or properly address apparent red flags, they may be in breach of legal or regulatory requirements. MSOs may also be exposed to civil and criminal liabilities as a result of their involvement in the associated ML activities.

---

1 News report by Xinhua News Agency
http://big5.www.gov.cn/gate/big5/www.gov.cn/lianbo/bumen/202407/content_6961469.htm

2 For the purpose of typology, "money exchange gangs" refers to illicit groups that unlawfully provide large-amount currency exchange services for individuals and entities, as well as offer high-interest loan services to gamblers in Macao. These illicit groups seek to circumvent the Mainland's regulations on foreign exchange controls and overseas debit card withdrawal limit, by illegally exchanging substantial amounts of Hong Kong dollars in cash for gamblers.

3 For the purpose of this circular, "third party" means any person other than the customer.

Purpose of this circular

The C&ED continually monitors anti-money laundering and counter-financing of terrorism ("AML/CFT") trends relating to the MSO sector and promulgates guidance and circulars from time to time as necessary to assist the sector in identifying suspicious transactions and remaining vigilant on risk trends. In connection with the vulnerabilities associated with the acceptance of payment from third parties, this circular serves to:

- remind MSOs of their existing obligations under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Chapter 615 ("AMLO") and Guideline on AML/CFT (For MSOs) ("AML/CFT Guideline");

- provide examples of the more common red flags/potentially higher risk factors identified to date; and

- set out the expected regulatory standards to facilitate MSOs' compliance in managing associated ML risks.

Obligations of MSOs

MSOs should pay heed to red flags/potentially higher risk factors and critically review and enhance their AML/CFT policies, procedures and controls (collectively referred to as "AML/CFT Systems") for the purpose of complying with relevant legal and regulatory requirements, including:

- section 5(1)(b) of Schedule 2 to the AMLO, requiring MSOs to continuously monitor their business relationship with customers by conducting appropriate scrutiny of transactions (cash and non-cash transactions) carried out for the customers to ensure that they are consistent with the MSO's knowledge of the customer and the customer's business, risk profile and source of funds;

- section 5(1)(c) of Schedule 2 to the AMLO, requiring MSOs to identify transactions that are complex, unusually large in amount or of an unusual pattern; and have no apparent economic or lawful purpose;

- section 23 of Schedule 2 to the AMLO, requiring MSOs to take all reasonable measures to ensure that proper safeguards exist to mitigate money laundering and terrorist financing ("ML/TF") risks and to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2 to the AMLO;

- paragraph 3.2 of the AML/CFT Guideline, requiring MSOs to put in place appropriate AML/CFT Systems to effectively manage and mitigate the risks that are relevant to the MSO and take enhanced measures to manage and mitigate the risks where higher risks are identified; and

- paragraph 4.4.5 of the AML/CFT Guideline, requiring MSOs to make appropriate enquiries about customers who are individuals, where there are indications that the customer is not acting on his own behalf.

Red flags/potentially higher risk factors

In general, if a transaction carries the name of a third party as the payer or otherwise does not appear to be consistent with the usual business/activity of the customer, the customer should be asked to provide further explanation of the nature of the remittance. MSOs should be vigilant in looking out for red flags/potentially higher risk factors that may arouse reasonable suspicion in MSOs or their staff of transactions for illegitimate purposes.

The following is a non-exhaustive illustrative list of red flags/potentially higher risk factors:

- transactions which are incompatible with the MSO's knowledge and experience of the customer in question or with the purpose of the relevant business transaction, for example, a mismatch between the economic activity, place of origin, or person and the remittances received/sent;

- multiple customers appear to be trying to avoid customer due diligence ("CDD") requirements to be conducted by the MSO and seem to be working together to break one transaction into two or more transactions below CDD thresholds;

- a concentration of seemingly unrelated customers that share the same transaction pattern (for example, transferring funds to a single individual's account);

- transfers of large sums of money to or from a place outside Hong Kong with instructions for payment in cash. The circumstances would be more suspicious if the originators or recipients are walk-in and non-resident customers instructing the MSO to carry out a single transaction;

- transactions which are carried out by the customer on behalf of a third party without an appropriate business relationship with such party;

- a large number of seemingly unrelated customers having authorised the same third party (who is not a regulated person or entity) to give instructions to the MSO to conduct various activities through the business relationship established;

- frequent or large fund transfers carried out by the customer which are funded by a third party without a credible commercial rationale or explanation; and

- customers who cannot immediately provide additional identification documents as required.

Expected standards on key control measures

MSOs are reminded to enforce appropriate and effective control measures which are capable of addressing these risks and meeting the requirements set out in the AMLO and relevant guidelines and circulars[4]. MSOs are required to take reasonable steps and implement robust AML/CFT Systems to learn about their customers, identify the beneficial owner of transactions, detect potential illegal activities, make prompt follow-up enquiries and report suspicious transactions where necessary.

The expected regulatory standards on key control measures are provided as follows to assist MSOs in reviewing the adequacy of their AML/CFT Systems for mitigating the risks associated with the use of third party payments for fund transfers:

- General

1. MSOs should critically assess the risk of being inadvertently exposed to crimes as well as legal and compliance risks. In particular, MSOs should take reasonable steps to identify and establish the true and full identity of each customer and beneficial owner, and give serious consideration to refusing third party payments.

2. MSOs which accept third party payments should put in place clear and detailed policies and procedures for scrutinising them and ensuring that the acceptance of third party payments is subject to stringent management approval. These AML/CFT Systems should be approved by senior management, effectively communicated to all relevant staff members and enforced through robust compliance monitoring programmes.

3. MSOs which are unable to put in place adequate control measures to mitigate the inherently high risks and meet the relevant regulatory requirements should not accept any third party payment.

- Policies and procedures

4. Third party payments should be accepted only under exceptional and legitimate circumstances and when they are reasonably in line with the customer's profile and normal commercial practices. These policies and procedures should be approved by senior management and address, among others:

   (a) the exceptional and legitimate circumstances under which third party payments may be accepted and their evaluation criteria;
   (b) the monitoring systems and controls for identifying transactions involving third party payments in the form of funds;[5]

---

[4] See also Supervisory Findings of Customer Due Diligence ("CDD") Related Issues dated 22 November 2023 and Money Laundering and Terrorist Financing Risks Associated with Delivery Channels dated 13 December 2021.

[5] For example, MSOs should obtain supporting documents (e.g. bank statements and advice slips) from customers to ascertain whether payments have come from third parties.

(c) if applicable, the due diligence process for assessing whether third party payments meet the evaluation criteria for acceptance;
(d) the enhanced monitoring of client accounts involving third party payments, and the reporting of any ML/TF suspicions identified to the Joint Financial Intelligence Unit ("JFIU"); and
(e) the respective designated managers or staff members responsible for carrying out these policies and procedures.

5. To facilitate the prompt identification of the sources of payments in the form of funds, MSOs are strongly encouraged to require their customers to designate bank accounts held in their own names for the making of all payments. This will make it easier for MSOs to ascertain whether funds have originated from their customers or to complete the necessary due diligence process to determine the acceptability of a third-party payer before effecting a third party payment.

- Due diligence process for assessing third party payments

6. Due diligence process for assessing third party payments should include:

(a) critically evaluating the reasons of and the need for third party payments;
(b) taking reasonable measures on a risk-sensitive basis to (i) verify the identities of the third parties; and (ii) ascertain the relationship between the third parties and the customers;
(c) obtaining approval from senior management with a relevant role at the MSO with respect to AML/CFT for the acceptance of a third party payment; and
(d) documenting the findings of enquiries made and corroborative evidence obtained during the due diligence process as well as the approval of a third party payment.

7. Given that not all third-party payers pose the same level of ML/TF risk,[6] MSOs should apply enhanced scrutiny to those third parties which might pose higher risks, and establish the relevant customer's or beneficial owner's source of funds[7] involved in the corresponding transactions.

---

[6] Examples of third parties that are generally considered to pose relatively low risks include immediate family members (e.g. a spouse, parent or child), beneficial owners or affiliated companies of the customers, or regulated financial institution. Other third parties pose higher risks.

[7] Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and the MSO (e.g. the amounts being invested, deposited, or wired/remitted as part of the business relationship). Source of funds information should not simply be limited to knowing from where the funds may have been transferred, but also the activity that has generated the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

8. MSOs should exercise extra caution when the relationship between the customer and the third party is hard to verify, the customer is unable to provide details of the identity of the third-party payer for verification before the payment is made, or a single third party is making or receiving payments for or from several seemingly unrelated customers.[8]

- Ongoing monitoring

9. Ongoing monitoring of transactions involving third party payments should be stepped up and MSOs should pay special attention to red flags relating to third-party transactions.[9] Identification of potentially suspicious transactions should prompt follow-up enquiries and further investigation. MSOs should be alert to the possibility that the third-party payer is the true beneficial owner, and the risks to which that may give rise. Suspicious transaction reports should be made to the JFIU when there are grounds for suspicion of ML or TF.

- Staff training, record keeping and client communication

10. Clear and sufficient guidance should be provided for the staff responsible for evaluating whether a third party payment is reasonable and meets the criteria for acceptance (including examples of acceptable third-party payers) as set out in the MSO's policies and procedures.

11. The findings of enquiries made and corroborative evidence obtained during the evaluation and approval of a third party payment should be properly documented.

12. MSOs should clearly inform customers of their policies for handling third party payments. These should include policies for rejecting third-party payments or accepting them under exceptional and legitimate circumstances, and requirements for customers to provide supporting documents to ascertain whether payments have come from third parties and verify third party payer information.

MSOs are strongly advised to review the advisory circulars issued by the C&ED, assess whether any enhancements are required for their AML/CFT Systems and adopt appropriate and effective control measures with a view to mitigating the risks associated with third party payments and meeting relevant obligations.

The C&ED will not hesitate to take enforcement actions, disciplinary sanctions and suspension or revocation of a licence, where appropriate, against MSOs for breach of statutory and regulatory requirements. All material issues and deficiencies identified in this regard will be investigated. These will include situations where there is reason to suspect that MSOs have knowingly facilitated third party payments as well as situations where it appears that they have failed to detect and act on any red flags, including inadequate procedures and controls.

---

[8] For example, MSO should further verify the identity of the third party with reference to additional identification documents, data or information that have not been previously used for verification purposes.

[9] Comprehensive red flags for third party payments should be defined in the MSOs' transaction monitoring system.

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