SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

17 November 2025

Circular to Licensed Corporations, SFC-licensed Virtual Asset Service Providers and Associated Entities

Anti-Money Laundering / Counter-Financing of Terrorism

Detection and prevention of potential layering activities in money laundering

1. The Securities and Futures Commission (SFC) has recently observed an emerging trend of illicit actors exploiting licensed corporations and virtual asset trading platforms for potential layering activities in money laundering. Failing to detect and prevent such activities poses grave money laundering and terrorist financing (ML/TF) risks to firms and the financial sector as a whole, enabling illicit actors to infiltrate legitimate channels and obscure the origins of potential crime proceeds.

2. Licensed corporations, SFC-licensed virtual asset service providers and associated entities (collectively referred to as "licensed firms") are reminded that strict adherence to their anti-money laundering and counter-financing of terrorism (AML/CFT) obligations is not only a regulatory requirement, but also essential for safeguarding the integrity of both their operations and the broader financial system.

3. The senior management of licensed firms, in particular, responsible officers (ROs), managers-in-charge (MIC) of overall management oversight and AML/CFT, the compliance officer and the money laundering reporting officer (MLRO), as well as the board of directors, are expected to be vigilant in fulfilling their responsibilities to implement effective AML/CFT policies, procedures and controls that can adequately address and manage the ML/TF risks identified.

4. The SFC issues this circular to analyse the major red flags identified in potential layering activities and reiterate our regulatory expectations on licensed firms regarding the establishment and implementation of effective AML/CFT measures to detect and prevent potential layering activities in money laundering.

Emerging trend of potential layering activities

5. From our supervisory work, the SFC has identified an emerging trend of suspicious fund movements involving frequent and swift fund deposits as well as withdrawals in client accounts maintained with licensed firms. A majority of the fund deposits made to these client accounts were not deployed for trading, but were, instead, withdrawn either immediately or within a short period of time.

6. These frequent and swift fund deposits and withdrawals suggested that the clients might use the accounts maintained with the licensed firms as depositary accounts or conduits for transfers, which could obscure the origin and destination of the funds and constitute layering activities in money laundering.

7. Potential layering activities typically exhibit the following patterns:

   (a) frequent and scattered fund deposits, sometimes in small or odd amounts with signs of smurfing[1], are made from multiple bank accounts held in the concerned clients' names through bank transfers. These deposits may occur within a few hours or a few days and/or outside regular banking hours;

   (b) the scattered fund deposits, after accumulating up to a certain amount, will be withdrawn to the concerned clients' bank accounts. While being held under the same clients' names, these bank accounts may be different from those originally used for the deposits. The withdrawal requests are likely made and/or processed on the same day or the following business day;

   (c) no trading activities, or only minimal trading activities that are not commensurate with the amount of deposits, have taken place in these concerned accounts during the entire period; and

   (d) most of the accounts remain inactive after all funds have been withdrawn.

8. Furthermore, recent intelligence shared by the Hong Kong Police Force also revealed an increasing number of client accounts maintained with licensed firms are being exploited for processing illicit proceeds arising from deception and scam cases to obscure fund flows. More specifically, it was noted that victims of these cases were instructed to make deposits to bank accounts of unknown parties. The funds were then layered through bank transfers to licensed firms and subsequently withdrawn to other bank accounts, or converted to virtual assets (VAs) through licensed firms that provide VA dealing or trading services and subsequently withdrawn to unhosted wallets. These layering activities, conducted through licensed firms, appear to be orchestrated to obscure the flow of funds.

9. The above suspicious patterns also suggest that the concerned accounts maintained with banks and licensed firms might be abused by clients who are illicit actors or stooges, or compromised by illicit actors for laundering crime proceeds.

Detecting red flags of suspicious transactions and activities indicating potential layering activities

10. Notwithstanding the above, the SFC noted that some licensed firms have failed to detect the apparent red flags exhibited in the aforementioned transaction patterns. In particular, some of them have disregarded the patterns of frequent and swift fund movements with no or minimal trading activities, solely on the basis that no third party was involved given the deposits and withdrawals appeared to be made through bank accounts or wallet addresses held by the clients.

11. In this regard, the SFC has conducted a detailed analysis of the potential layering activities to identify the red flags exhibited in the transactions. Most of the red flags identified are already incorporated in the lists of non-exhaustive illustrative indicators of

[1] Smurfing is a common technique in money laundering where large sums are deliberately broken down into smaller and less suspicious or noticeable transactions.

suspicious transactions and activities in the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) (AML/CFT Guideline)[2]. In particular:

(a) clients used licensed firms to make payments or hold funds that are rarely used, or are not being used, for trading as if the account appears to be used as a depositary account or a conduit for transfers (as illustrated in paragraph 7 above, fund deposits and withdrawals are made with no or minimal trading activities conducted);

(b) transactions appear to be undertaken in a structured and sequential manner in order to avoid exceeding the transaction monitoring thresholds (as illustrated in paragraph 7(a) above, frequent and scattered deposits sometimes structured in small or odd amounts);

(c) clients entered a business relationship with licensed firms only for a single transaction or for a very short period without a reasonable explanation (as illustrated in paragraph 7(d) above, the accounts remain inactive after all funds have been withdrawn);

(d) clients frequently changed bank account details (eg, clients registered multiple bank accounts for deposits and other bank accounts solely for withdrawal; the number of bank accounts registered was unreasonably high);

(e) clients made transfers to and from jurisdictions which were not consistent with their declared business dealing or interests (eg, clients deposited funds from an account maintained with a bank neither incorporated nor operating in a jurisdiction where the clients reside, nor in Hong Kong);

(f) transaction sizes or patterns were not in line with the background of the clients (eg, clients deposited substantial amount of funds, securities or VAs that were incommensurate with their financial profiles declared in the account opening documents);

(g) profile details of clients were associated with other apparently unrelated clients (eg, multiple clients shared the same bank account for fund withdrawals, each providing seemingly legitimate documents to demonstrate the ownership of the bank account);

(h) conversion of funds into VAs with no logical or apparent reason which obscures the fund flow (eg, frequent and scattered fund deposits were converted into VAs and subsequently withdrawn in whole immediately, leaving the account inactive thereafter; buying and selling of VAs with no discernible purpose or where the nature, size or frequency of the transactions appears unusual); and

(i) apparently unrelated clients entered the licensed firm's platform from the same IP address or device identifier (eg, multiple clients shared the same IP address and/or device to access the mobile application or web-based platform of the licensed firms for executing transactions or other activities).

[2] Paragraph 12.16 of and Appendix B to the AML/CFT Guideline.

Implementing effective AML/CFT measures to detect and prevent layering activities

12. The SFC wishes to reiterate that failure to implement proper AML/CFT measures in compliance with regulatory requirements allows illicit actors to exploit legitimate channels and obscure the origins and destinations of criminal proceeds, which poses grave risks to the broader financial system.

13. Licensed firms are reminded of their AML/CFT obligations and the importance of upholding essential safeguards against ML/TF to detect and prevent layering activities. Licensed firms must ensure the implementation of robust and effective transaction monitoring systems and processes, and exercise heightened vigilance when processing deposits and withdrawals for their clients.

14. Upon detection of any red flags of suspicious transactions and activities, licensed firms should conduct reviews and investigations promptly, having regard to the customer due diligence profile and historical transaction patterns of the clients, to assess whether there are grounds for knowledge or suspicion of ML/TF which may warrant filing of suspicious transaction reports to the Joint Financial Intelligence Unit (JFIU). Licensed firms should also conduct appropriate review of business relationships, consider the risks and impose appropriate controls to mitigate the risks identified[3]. For example, they should conduct appropriate review to assess whether other clients and their transactions exhibit similar red flags.

(A) Implementing robust and effective transaction monitoring systems and processes

15. Licensed firms should establish and implement adequately robust and effective systems and processes to monitor their clients' transactions and activities conducted[4]. In particular, the design, degree of automation and sophistication of the systems should be proportionate to the volume of transactions processed by and the ML/TF risk posed to the licensed firms. They should also regularly review the robustness and effectiveness of these systems and processes, including the parameters and thresholds adopted, to ensure that they remain appropriate for the licensed firm's operations and context, and can detect unusual or suspicious transactions or activities as intended[5].

16. The transaction monitoring systems and processes should enable licensed firms to detect the patterns indicative of the potential layering activities, including those set out in paragraphs 7, 8 and 11 above for further review and investigation. In particular:

    (a) the transaction monitoring systems should enable a licensed firm to identify a client who makes deposits and withdrawals of funds or VAs with no or minimal trading activities in between. The design of relevant thresholds and parameters should take into account the timing, size and amount of the deposits, withdrawals and any trading activities conducted by the clients. For example, if a client attempts to circumvent the monitoring thresholds by conducting minimal trading activities a week before depositing a significant amount of funds which is subsequently withdrawn without

[3] Paragraphs 7.20 and 7.29 of the AML/CFT Guideline.
[4] Paragraph 5.4 of the AML/CFT Guideline.
[5] Paragraphs 5.7 and 5.8 of the AML/CFT Guideline.

trading, the design of the thresholds and parameters should ensure that these suspicious fund movements are detected;

(b) the monitoring scenarios should enable a licensed firm to identify deposits and withdrawals conducted by clients in a structured manner (in particular, the deposits and withdrawals that appear to be structured in smaller or odd amounts and/or are conducted during odd hours);

(c) the monitoring scenarios should enable a licensed firm to identify a client who conducts deposits and withdrawals of funds or VAs only for a very short period with the account being inactive thereafter;

(d) changes in bank account details, or wallet address details in the case of VA, should be subject to appropriate scrutiny, having regard to the control procedures when processing deposits and withdrawals for clients set out in paragraphs 19 and 20 below;

(e) transfers to and from jurisdictions outside Hong Kong should be subject to appropriate scrutiny, in particular, when a client requests to deposit from or withdraw to an account maintained with a bank or VA service provider located in a place that does not appear to be in line with the client's nationality, or place of business operations or residence;

(f) the monitoring scenarios should enable a licensed firm to identify a client who conducts transactions that are incommensurate with the background of the client;

(g) sharing of bank accounts, or wallet addresses in the case of VA, among clients, especially unrelated clients, for deposits and withdrawals should be promptly identified;

(h) the thresholds and parameters should enable a licensed firm to detect scenarios such as multiple conversions of funds into VAs, or vice versa, within a very short period of time, and immediate withdrawal of the converted VAs or funds, which may indicate that the transactions were conducted solely for obscuring the fund flows; and

(i) for licensed firms with clients who predominantly trade online, the IP addresses and device identifiers used by clients to access the mobile application or web-based platforms should be subject to appropriate scrutiny to enable the identification of apparently unrelated clients who share the same IP address or device, which may indicate potential collusion among clients or stooges acting in concert.

17. Furthermore, when conducting VA-related activities, licensed firms should ensure that VA transactions and associated wallet addresses are subject to screening by employing appropriate technological solutions (eg, blockchain analytical tools) to identify the source and destination of the VAs prior to conducting the transactions for their clients. Subsequent screening of the VA transactions and associated wallet addresses should also be conducted on a risk-sensitive basis after conducting the transactions. Any

transactions involving wallet addresses that are directly and/or indirectly associated with illicit or suspicious activities, such as fraud, should be appropriately followed up[6].

(B) Exercising heightened vigilance when processing deposits and withdrawals for clients

18. Licensed firms must take all reasonable measures to ensure that proper safeguards exist to mitigate ML/TF risks[7]. To prevent the facilitation of layering activities, licensed firms should exercise heightened vigilance when processing deposits and withdrawals in the form of funds and VAs for their clients. Specifically, the monitoring of transaction patterns as well as the processing of deposits and withdrawals should be conducted in a holistic manner. In particular, the acceptance of deposits and release of payments should take into account the red flags of suspicious transactions or activities detected in the transaction monitoring process.

19. While licensed firms generally do not accept third-party deposits and payments[8], they are still required to establish robust controls to help detect and prevent the layering activities, particularly those illustrated in paragraphs 7 and 8, when processing deposits and withdrawals through bank accounts[9], or wallet addresses in the case of VAs, owned by the clients.

Establishing registration or whitelisting mechanism for bank accounts or wallet addresses

20. To facilitate the ongoing monitoring of client deposits and withdrawals and to detect the red flag on frequent changes of bank account or wallet address details[10], licensed firms are expected to establish a registration mechanism for bank accounts used by clients for depositing and withdrawing funds through bank transfers, or a whitelisting mechanism for wallet addresses used by clients for depositing and withdrawing VAs. Under the bank account registration or wallet address whitelisting mechanism, licensed firms should:

    (a) take reasonable measures[11] to ascertain the ownership of the bank accounts. In the case of VA, ensure that the ownership of wallet address has been ascertained by appropriate measures such as micropayment test and message signing test. Licensed firms should avoid complete reliance on the documents provided by clients to verify the ownership without performing additional steps to ascertain the authenticity of the documents;

---

6 Paragraphs 12.7 and footnote 128 of the AML/CFT Guideline.

7 Section 23(b) of Schedule 2 to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) and paragraph 1.24 of the AML/CFT Guideline.

8 This circular focuses on the controls in relation to deposits and withdrawals through bank accounts and wallet addresses owned by clients. For third-party deposits and payments, please refer to the requirements stipulated in Chapter 11 and paragraph 12.10 of the AML/CFT Guideline.

9 For the avoidance of doubt, for clients onboarded via the "online onboarding of clients using a designated bank account in Hong Kong", licensed firms should conduct all deposits and withdrawals for the client's trading account through the Designated Bank Account(s) only. For details, please refer to the SFC's acceptable account opening approaches.

10 Paragraph 5(k) of Appendix B to the AML/CFT Guideline.

11 These may include requiring clients to set up Electronic Direct Debit Authorisation (eDDA) or bank-securities transfer arrangements for their registered bank accounts, or require them to deposit funds and check the names of the deposit records.

(b) set limits on the number of bank accounts or wallet addresses registered or whitelisted by clients for deposits and withdrawals on a reasonable and need basis to facilitate monitoring and prevent clients from using multiple bank accounts or wallet addresses for depositing funds or VAs and other bank accounts or wallet addresses for withdrawing funds or VAs to obscure fund flows;

(c) ensure any addition or replacement of registered bank accounts or whitelisted wallet addresses is subject to review and approval by the licensed firm's senior management (eg, MIC of AML/CFT, compliance officer or MLRO) in a risk-sensitive manner, considering factors such as the frequency of changes to bank account or wallet address details as well as client deposit and withdrawal patterns; and

(d) prohibit the sharing of bank accounts or wallet addresses among clients[12], including prior registered bank accounts or whitelisted wallet addresses that have been removed or replaced by clients.

Exercising appropriate scrutiny on withdrawal requests and implement reasonable measures to mitigate the risk of facilitating layering activities

21. Licensed firms should exercise appropriate scrutiny when processing withdrawal requests, especially for immediate withdrawals that are made through newly registered bank accounts or newly whitelisted wallet addresses to detect clients who register or whitelist a different bank account or wallet address for withdrawals with no discernible purpose. This may be conducted solely for the purpose of obscuring fund flows.

22. Upon detection of red flags of suspicious transactions and activities, licensed firms should conduct thorough investigations to assess whether such suspicions warrant reporting to the JFIU. Licensed firms should process the withdrawal requests only when there is no suspicion of ML/TF.

23. Licensed firms are also expected to implement reasonable measures to mitigate the risk of facilitating layering activities when processing withdrawal requests[13], especially when the deposited funds or VAs are not substantially deployed for trading and with no discernible purpose. These may include:

(a) limiting withdrawals to the bank accounts or wallet addresses from which the funds or VAs were originally deposited; and

(b) implementing a withdrawal holding period (eg, one to two days) subsequent to client deposits to prevent immediate withdrawals.

---

[12] Except for circumstances where clients of a licensed firm share a jointly-owned bank account and the licensed firm has applied policies and procedures for handling deposits and payments through such jointly-owned bank account accordingly. For details, please refer to Q26 of the FAQ on AML/CFT.

[13] Licensed firms are reminded to comply with all applicable laws and regulations when dealing with clients' property. In particular, pursuant to section 25 of the Organized and Serious Crimes Ordinance (Cap. 455) and the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap.405), a person commits an offence if he deals with any property while knowing or having reasonable grounds to believe that the property represents any person's proceeds of an indictable offence or drug trafficking.

24. The SFC remains fully committed to upholding the integrity of Hong Kong's financial system and continues to supervise licensed firms' compliance with applicable AML/CFT requirements through on-site inspections, offsite monitoring and thematic reviews.

25. The SFC will not hesitate to exercise its powers under the Securities and Futures Ordinance and the AMLO to take appropriate regulatory actions against licensed firms and their senior management, including relevant directors, ROs, MIC and MLRO, for failing to discharge their AML/CFT obligations. These include appropriate supervisory interventions such as imposing licensing conditions, limiting the licensed firms' business and activities (eg, prohibition of transactions or new client onboarding), or taking enforcement actions against the licensed firms and relevant personnel such as appropriate disciplinary actions (eg, licence revocation or suspension, pecuniary fine and reprimand).

26. Should you have any queries regarding the contents of this circular, please contact Ms Kiki Wong at 2231 1569 who will assist in referring your queries to the relevant officer.

Intermediaries Division
Securities and Futures Commission

End

SFO/IS/038/2025