

## Key control measures and examples of effective practices

### General

1. Firms which accept third-party deposits or payments should put in place clear and detailed policies and procedures for scrutinising them and ensure that the acceptance of a third-party deposit or payment is subject to stringent management approval. These policies, procedures and controls should be approved by senior management<sup>1</sup>, effectively communicated to all relevant staff members and enforced through robust compliance monitoring programmes.
2. Nevertheless, firms should adopt a policy which discourages third-party deposits and payments and only accept them under exceptional and legitimate circumstances having regard to the client's profile and normal commercial practices. The acceptance of a third-party deposit or payment should be approved by the MIC of AML/CFT or MLRO<sup>2</sup>, and where the deposit or payment involves a third-party payor or payee who might pose higher risks (see paragraph 9 below), it should be subject to a dual approval process<sup>3</sup>.
3. Firms which are unable to put in place adequate control measures to mitigate the inherently high risk and meet the relevant compliance requirements should not accept any third-party deposits or payments.

### Third-party deposits

#### *Policies and procedures*

4. Firms should clearly define, in policies and procedures approved by senior management (see paragraph 1 above), the exceptional and legitimate circumstances (including examples of acceptable third-party payors) under which third-party deposits may be accepted, set out the control measures to be carried out before accepting any such deposits and designate the managers and staff members responsible for carrying out these control measures.
5. Firms should put in place effective monitoring systems and controls to identify third-party deposits into their bank accounts and deal with them in accordance with their policies and procedures. For example, firms may obtain supporting documents from clients to ascertain whether deposits have come from third parties.

---

<sup>1</sup> The senior management of an LC or AE, which is obliged under the AML Guideline to satisfy itself that the business is taking sufficiently effective measures to protect itself against the risks of ML/TF, should approve these policies and procedures.

<sup>2</sup> A standing approval may be given for a particular third-party payor or payee; however, it should be subject to review periodically or upon the occurrence of a trigger event (eg, when a third-party deposit or payment transaction which is unusual or not in line with the firm's knowledge of the client takes place).

<sup>3</sup> For effective internal control, dual approval by the officer holding the position of MIC of AML/CFT or MLRO and another member of senior management should be required. Any standing approval should be subject to review periodically or upon the occurrence of a trigger event.

6. Rejected third-party deposits should be returned to their payment sources as soon as practicable<sup>4</sup>.

*Due diligence and evaluation*

7. Due diligence on any third-party deposit should be conducted to determine: (a) the identity of the third-party payor; (b) the relationship between the client and the third-party payor; and (c) the reason for receiving the deposit from the third party.
8. Firms should take reasonable measures on a risk-sensitive basis to verify the identities of third-party payors and ascertain their relationships with clients. Third-party payors generally considered to pose relatively low risks include immediate family members (eg, a spouse, parent or child), beneficial owners and affiliated companies of corporate clients and regulated custodians and lending institutions.
9. Other third-party payors might pose higher risks and if firms permit them to make deposits, they should be subject to enhanced scrutiny. Firms should exercise extra caution when the relationship between the client and the third-party payor is hard to verify, the client is unable to provide details of the identity of the third-party payor for verification before the deposit is made or one third-party payor is making payments for several seemingly unrelated clients<sup>5</sup>.
10. Firms should critically evaluate the reasons and the need for third-party deposits. They should take all appropriate measures (eg, making further inquiries with the clients and obtaining corroborative evidence from relevant sources) to ensure that a third-party deposit is reasonably in line with the client's profile and normal commercial practices (including the frequency and pattern of previous third-party deposits)<sup>6</sup> before accepting the payment and crediting it to the client's ledger account as available funds.

*Ongoing monitoring*

11. Ongoing monitoring of client accounts involving third-party deposits should be stepped up and firms should pay special attention to red flags relating to third-party transactions<sup>7</sup>. Identification of potentially suspicious transactions should prompt further investigation. Firms should be alert to the possibility that the third-party payor is the true beneficial owner, and the risks which that may give rise to. A suspicious transaction report should be made to the JFIU when there are grounds for suspicion of ML or TF.

---

<sup>4</sup> Firms should ensure that a standing authority or written direction is obtained from the client to return any rejected third-party deposit to its source (sections 4 to 8 of the Securities and Futures (Client Money) Rules (Client Money Rules)). Firms are also reminded to comply with the Client Money Rules and pay any money received on behalf of a client in the course of or in relation to the conduct of any regulated activity into a segregated account within one business day even if due diligence and approval process are yet to be completed (Section 4(4)(a) of the Client Money Rules).

<sup>5</sup> In a similar vein, firms should be alert to the possibility that several unrelated clients authorising the same third party to give trading instructions for their accounts could be an indication of illicit activities or efforts to conceal beneficial ownership. They should conduct proper due diligence and ongoing monitoring to mitigate any financial crime and compliance risks.

<sup>6</sup> Examples include that the client would fail to meet a margin call deadline or settlement obligation if the funds from the third party were first deposited into the client's bank account and then transferred to the LC's bank account; or a new client who has not yet opened a bank account in Hong Kong.

<sup>7</sup> Examples of such red flags are provided in paragraphs 7.12 to 7.14 of the AML Guideline. Comprehensive red flags for third party deposits should be defined in the firm's transaction monitoring system. Closer monitoring should be applied to deposits from third parties who are not beneficial owners of the clients, regulated custodians or lending institutions.

### Third-party payments

12. Requests from clients for third-party payments should normally be refused. The need for a third party, and not the client, to receive a client's funds should be rare<sup>8</sup>. Firms should weigh financial crime and compliance risks when deciding whether to accept such a request.
13. Firms which decide to accept third-party payment requests should clearly define, in policies and procedures approved by senior management (see paragraph 1), the exceptional and legitimate circumstances (including examples of acceptable third-party payees) under which third-party payment requests may be accepted<sup>9</sup>, and set out the control measures<sup>10</sup> to be carried out before accepting any such payment request. They should also designate the managers and staff members responsible for carrying out these control measures.
14. Due diligence on any third-party payment request should be conducted to determine: (a) the identity of the third-party payee; (b) the relationship between the client and the third-party payee; and (c) the reason for making the payment to the third party.
15. Firms should apply the relevant measures for due diligence and ongoing monitoring of client accounts set out in paragraphs 8 to 11 above, with the appropriate substitution of "third-party deposit" with "third-party payment" and "payor" with "payee".

### Designated bank accounts

16. Firms are strongly encouraged to require their clients to designate bank accounts held in their own names or the names of acceptable third parties for the making of all deposits and withdrawals<sup>11</sup>. This will make it easier for firms to complete the necessary due diligence to determine the acceptability of a third-party payor or payee before effecting a third-party deposit or payment.
17. This procedure will also make it easier for firms to ascertain whether deposits have originated from their clients or acceptable third parties. For example, firms can check their bank statements and advice slips to determine if a deposit was made from a designated bank account.

---

<sup>8</sup> Examples include where a client enters into a service agreement under which the proceeds of the sale of securities are transferred to a third-party custodian or margin financier; a client requests the firm to effect payments for fees and charges under service agreements with a third-party asset manager which manages the client's investment portfolio in a securities account maintained with the firm; and a client requests the firm to draw from his account to pay the seller or deposit funds into an escrow agent's account for the purchase of listed shares or bonds off-exchange.

<sup>9</sup> Given that the need for third-party payments should be rare and normal commercial practices may differ, circumstances which may be considered to be exceptional and legitimate for third-party payments may not be the same as or similar to those for third-party deposits.

<sup>10</sup> Any request for third-party payment should always be supported by a written direction or standing authority from the client in accordance with section 5 of the Client Money Rules.

<sup>11</sup> For the avoidance of doubt, where a client has been on-boarded online using non-face-to-face procedures provided in the SFC's circular dated 12 July 2018, the firm should conduct all deposits and withdrawals for the client's trading account through a designated bank account held in the client's name.

Staff training, record keeping and client communication

18. Clear and sufficient guidance should be provided to the staff responsible for evaluating whether a third-party deposit or payment is reasonable and meets the criteria for acceptance (including examples of acceptable third-party payors and payees) as set out in the firm's policies and procedures.
19. The findings of inquiries made and corroborative evidence obtained during the evaluation and approval of a third-party deposit or payment should be properly documented.
20. Firms should clearly inform clients in writing of their policies for handling third-party deposits and payments. These should include policies for rejecting third-party deposits or accepting them under exceptional and legitimate circumstances, requirements for clients to provide supporting documents to ascertain whether deposits have come from third parties and verify third-party payor or payee information, and procedures for returning rejected third-party deposits.