



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B10/1C
B1/15C

12 December 2025

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Guidance on combating high-end money laundering

I am writing to share the Hong Kong Monetary Authority (HKMA)'s observations regarding evolving money laundering and terrorist financing (ML/TF) typologies that involve the use of sophisticated methods in an attempt to circumvent the anti-money laundering and counter-financing of terrorism (AML/CFT) controls of financial institutions (referred to as "high-end money laundering").

In some of these cases, criminal syndicates established customer relationships in the retail banking segment as a gateway to gain access to the banking system and subsequently used that access to move large amounts of funds across multiple accounts, including accounts in retail wealth management and private banking segments. In another line of cases, criminals opened accounts using nationalities acquired from jurisdictions which offered citizenship through investment programmes, and established customer relationships with the same financial institution across multiple jurisdictions with a view to facilitating cross-border fund transfers.

In light of these evolving ML/TF typologies, the HKMA conducted a thematic review to assess the adequacy and effectiveness of Authorized Institutions (AIs)' AML/CFT controls in mitigating the ML/TF risks associated with high-end money laundering. The review revealed that AIs had in general established adequate and effective AML/CFT controls, however, some areas for enhancement were identified.

1. Understanding of ML/TF risks

While the review noted that AIs' customer risk assessment frameworks were generally capable of identifying customer relationships with higher ML/TF risks, there was room for improvement in some AIs' implementation of these frameworks in order to respond to the evolving and increasingly sophisticated methods used by criminal syndicates. In particular, AIs should ensure that they

adequately understand and assess the reasonableness of certain customer characteristics (e.g. multiple nationalities) and/or material changes in customer profiles (e.g. employment, wealth contributor, assets under management) which may have implications for the ML/TF risk profiles of customer relationships, and apply effective additional controls proportionate to those risks. Particular attention should be given to flagging and escalating cases where multiple risk indicators are present. 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)

All AIs reviewed had established CDD policies and procedures which generally met the legal and regulatory requirements. However, certain areas for improvement were noted regarding the effective implementation of CDD measures proportionate to the ML/TF risks associated with customer relationships. For example, in some cases significant differences were noted in the level of CDD undertaken between high-net-worth customers in the retail wealth management segment and private banking customers, with private banking customers being subject to noticeably more robust and effective requirements, despite the fact that the ML/TF risk exposures in the two segments were very similar. AIs should periodically monitor the portfolios of retail high-net-worth customers and apply additional CDD measures proportionate to the associated ML/TF risks, taking into account any changes in the risk profiles of customers.

3. Establishment and corroboration of source of wealth (SoW) and source of funds (SoF)

The establishment and corroboration of SoW and SoF is a key preventive control which, if implemented effectively in line with risk-based principles, can help to mitigate higher ML/TF risks. While in general AIs had implemented policies and procedures meeting legal and regulatory requirements, the review noted a few cases where the AI's front-line staff did not possess sufficient risk awareness and experience in handling higher-risk situations. This resulted in an overreliance on customer representations when establishing SoW and SoF, without seeking clarification regarding ambiguities, challenging the reasonableness of the information provided, or obtaining additional documentation for corroboration. The compliance function of AIs should provide front-line staff with sufficient operational guidance and support for the effective handling of higher-risk customer relationships, referencing relevant guidance issued by the HKMA and the Hong Kong Association of Banks¹.

4. Transaction monitoring (TM)

¹ These include relevant guidance issued by the HKMA such as the "Smart Tips for Private Banking - Establishment of SoW and SoF" dated 7 March 2023 and the circular on "Effective Execution of Risk-based Approach for CDD" dated 8 February 2024, as well as Appendix 1 "Establishing SoW" to the Frequently Asked Questions in relation to AML/CFT developed by the Hong Kong Association of Banks.

The TM systems of all AIs reviewed were able to identify and generate alerts for unusual or suspicious transactions. However, the review noted that certain TM alerts were closed without sufficient justification and analysis, including, for example, some alerts triggered by large deposits from opaque sources such as cash or cashier's orders, significant transactions with third parties whose relationships with the customer were not always adequately understood, and transactions with jurisdictions that had no apparent nexus to the customer relationship. AIs should adequately assess the reasonableness of transactions taking into account the customer risk profiles and historical transactions.

5. Sharing of information among banking affiliates

To better prevent and detect ML/TF risks, some AIs had established mechanisms to share information concerning customer relationships presenting higher-risk indicators among affiliates of their banking groups operating in different jurisdictions. Such an approach enables a more holistic view of customer relationships, thereby facilitating the identification of potential ML/TF risks and the implementation of appropriate risk mitigating measures.

AIs should review their existing AML/CFT controls through a gap analysis and give consideration to optimising AML/CFT controls based on the areas for enhancement outlined above. The HKMA will continue to engage closely with the industry and provide further guidance where appropriate.

If AIs have any questions on this circular, they may approach their usual supervisory contact at the HKMA's AML and Financial Crime Risk Division.

Yours faithfully,

Raymond Chan
Executive Director (Enforcement and AML)