



DPSB/AML/2024/05
27 November 2024

Circular

Anti-Money Laundering and Counter-Financing of Terrorism Measures

Suspicious Transaction Report

Statutory Requirements for Suspicious Transaction Reporting

It is a statutory obligation under the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 (“DTROPO”)¹, the Organized and Serious Crimes Ordinance, Cap. 455 (“OSCO”)², as well as the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (“UNATMO”)³, that where a person knows or suspects that any property: (i) in whole or in part directly or indirectly represents any person’s proceeds of, (ii) was used in connection with, or (iii) is intended to be used in connection with drug trafficking or an indictable offence; or that any property is terrorist property, the person shall as soon as it is reasonable for him to do so, disclose that knowledge or suspicion to an authorized officer⁴.

In this regard, the Joint Financial Intelligence Unit (“JFIU”), formed up by the Hong Kong Police Force and the Customs and Excise Department (“C&ED”), is designated to administer the suspicious transaction reporting regime in Hong Kong and process the data and information collected in accordance with the above statutory requirements.

Please be reminded that any person, including both Category A and Category B registrants (“PMS Registrants”)⁵, is obligated to report such knowledge or suspicion to the JFIU through a suspicious transaction report (“STR”). Any failure to report such knowledge and suspicion carries a maximum penalty of imprisonment for three months and a fine of \$50,000.

As such, PMS Registrants should take steps to comply with the statutory requirements, in particular establishing the relevant policies as well as internal procedures for reporting suspicious transactions, and identifying the circumstances (commonly known as red flag indicators) for suspicious money laundering and terrorist financing (“ML/TF”) activities in the course of their business operation.

The “SAFE” Approach

PMS Registrants may consider adopting the “SAFE” approach as recommended by the JFIU, which draws out a systematic and practical mechanism to effectively identify suspicious

¹ Section 25A(1) of the DTROPO at <https://www.elegislation.gov.hk/hk/cap405>.

² Section 25A(1) of the UNATMO at <https://www.elegislation.gov.hk/hk/cap455>.

³ Section 12(1) of the UNATMO at <https://www.elegislation.gov.hk/hk/cap575>.

⁴ The authorized officer means any police officer, any member of the Customs and Excise Service established by section 3 of the Customs and Excise Ordinance, and any other person authorized in writing by the Secretary for Justice.

⁵ Category A or B registrant is the dealer in precious metals and stones which granted approval for the registration with the C&ED in accordance with Part 5C of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615.



transactions and ensure the submitted STRs of good quality. The “SAFE” approach proposes four key steps, which are:

- (1) Screening the account for suspicious indicators (i.e. red flag indicators): Recognition of a suspicious activity indicator or indicators;
- (2) Asking the customers appropriate questions;
- (3) Finding out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected; and
- (4) Evaluating all the above information: Is the transaction suspicious?

PMS Registrants may visit the JFIU’s website for more details on the application of the “SAFE” approach⁶.

Red Flag Indicators

The red flag indicators present the circumstances that could be suspicious in nature and associated with ML/TF activities, which may serve as a basis for consideration in identifying suspicious transactions. To effectively fulfil the reporting obligation, PMS Registrants should work out their own set of red flag indicators, so that relevant staff can have a clear understanding of the circumstances that should trigger the suspicious transaction reporting process. PMS Registrants may also consider to adopt the following examples of red flag indicators:

Examples of Red Flag Indicators	
■	For the customer due diligence (“CDD”) and record-keeping purposes, the customer is unable or unwilling to provide relevant information and document for his/her identity and/or the identity of the beneficial owner(s).
■	Purchase of the precious metals and stones (“PMS”) through multiple cash transactions over a short time period, and the cumulative amounts exceeds the statutory threshold for the CDD requirement, i.e. HK\$120,000.
■	The customer appears to be in a hurry to complete the transaction and/or does not care about the value, size and/or specification of the PMS or any other costs in the transaction.
■	The transaction is inconsistent with the profile of the customer. For example, the customer claimed to be a student or a domestic helper, but pays a large amount of cash for the PMS transaction or offers to sell high-value PMS items.
■	Regular customer significantly increases the purchase of PMS, e.g. bullion and loose diamond, or purchases the PMS unrelated to their main business, for no reasonable explanation.

⁶ The “SAFE” approach recommended by the JFIU at <https://www.jfiu.gov.hk/en/str.html>



Examples of Red Flag Indicators

- New customer offers a large amount of PMS items for sale, e.g. gold or diamond jewelry, where the source of the PMS is unknown or questionable.
- The PMS is offered at a rate significantly lower than their market value.
- The transaction involves third parties either as payers or recipients of payment or products for no apparent business purpose. For example, the customer requires that the PMS are delivered or the funds are paid to a third party.
- The customer cancels the PMS transaction shortly after deposit or full payment is made and requests a refund. For example, the customer pays cash for the PMS transaction and then requests a refund via bank transfer or cheque.
- Overpayment of a transaction with a request to refund the excess in cash or to a third party.
- The customer requires the PMS to be shipped through or to a country or territory that is designated as 'high risk for money laundering or terrorism activities' for no apparent economic reason.
- The customer appears to be related to a high-risk country or territory or entity that is associated with money laundering or terrorism activities or a person that has been designated as terrorists.
- Adverse news from the media or other open sources indicate that the customer is suspected of being involved in illegal activities, in particular the cases related to ML/TF.

Note to PMS Registrants

Please be reminded that once knowledge or suspicion has been formed, PMS Registrants should file an STR with the JFIU even where no transaction has been conducted. Furthermore, the above examples of red flag indicators are not exhaustive but reflect some suspicious circumstances related to the ML/TF activities, and in most cases, they may result from the situations of high ML/TF risk⁷. As such, PMS Registrants should regularly review the relevant policies and procedures to ensure the reporting mechanisms have taken into account the latest ML/TF developments and risk situations in the sector.

⁷ For identifying the high-risk situations, please refer to the circular issued by the C&ED, namely Anti-Money Laundering and Counter-Financing of Terrorism Systems with Risk-based Approach (For Category B Registrant), at: https://www.drs.customs.gov.hk/information/7121_circularsAndPublications



The JFIU e-reporting System

PMS Registrants may submit an STR to the JFIU via the e-reporting system, namely STREAMS⁸, which is only accessible by the registered users. Through the STREAMS, the registered users can also gain access to the STR analysis report released by the JFIU, which provides the latest ML/TF trend and typologies in relevant sectors on a quarterly basis. It is therefore recommended that PMS Registrants should register with the STREAMS so as to maintain a direct and effective e-reporting channel and be regularly updated with the ML/TF landscape.

Reference Materials

In addition, PMS Registrants are encouraged to refer to the JFIU publication, namely Strategic Analysis Report on Dealers in Precious Metals and Stone⁹, which covers the ML/TF trend in the PMS business sector in Hong Kong, and provides the case typologies and red flag indicators related to the ML/TF activities in the sector.

Please also note that the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (“AML/CFT”) (For Category B Registrants Dealing in Precious Metals and Stones) (“*Guideline on AML/CFT*”)¹⁰ issued by the C&ED, provides practical guidance to Category B registrants to establish their own effective AML/CFT systems (i.e. policies, procedures and controls)¹¹. Among others, chapter 7 of the *Guideline on AML/CFT* requires the reporting mechanism for suspicious transactions, and in fact this is also applicable to the business entities of relevant sectors including Category A registrants, particularly for formulating the policies and internal procedures in this regard.

For more details about the suspicious transaction reporting measures, PMS Registrants may refer to the information of JFIU website¹² and chapter 7 of the *Guideline on AML/CFT*.

Should you have any queries, please contact us at 5972 6086.

Dealers in Precious Metals and Stones Supervision Bureau Customs and Excise Department

⁸ The Suspicious Transaction Report and Management System (“STREAMS”) at: <https://www.jfiu.gov.hk/en/sbsal.html>

⁹ Website at https://www.jfiu.gov.hk/info/doc/SAR_ON_DPMS.pdf

¹⁰ Website at https://www.drs.customs.gov.hk/download/drsguideline/AML_CFT_Guideline_en.pdf

¹¹ According to section 23 of schedule 2 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap.615, category B registrant should implement an effective AML/CFT system covering all reasonable measures to mitigate the ML/TF risks and comply with the statutory requirements for customer due diligence and record-keeping measures.

¹² Website at https://www.jfiu.gov.hk/en/str_main.html