Anti-Money Laundering and Counter-Terrorist Financing Guideline for

Dealers in Precious Metals and Stones

(2018)

Anti-Money Laundering and Counter-Terrorist Financing Guideline for Dealers in Precious Metals and Stones (2018)

CONTENTS

Page

1. Introduction

1.1 The Financial Action Task Force ("FATF") is an inter-governmental body setting international anti-money laundering and counter-financing of terrorism ("AML/CFT") standards through its 40 Recommendations for compliance by member jurisdictions, including Hong Kong.

1.2 Since June 2003, dealers in precious metals and stones ("DPMS") have been classified as one of the designated non-financial businesses and professions ("DNFBPs") by FATF and are therefore subject to the same requirements in terms of AML/CFT measures as casinos, real estate agents, lawyers, accountants, and trust or company service providers ("TCSPs").

1.3 Customer due diligence ("CDD") and record-keeping requirements are the main strands of an effective AML/CFT regime to deter and disrupt money laundering ("ML") and terrorist financing ("TF") activities. FATF recommends that financial institutions and DNFBPs that engage in specified transactions[1] should implement CDD measures to identify and verify customers and beneficial owners, and maintain records on CDD and transactions for at least five years.

1.4 Starting from 1 March 2018, the statutory requirements under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("AMLO") (Cap. 615) to carry out CDD and record-keeping requirements have been extended to four DNFBPs, namely accounting professionals, legal professionals, estate agents, and TCSPs when they engage in specified transactions.

1.5 DPMS are not covered under the AMLO for the moment. However, according to international typologies and local ML cases, DPMS also face ML/TF risks. To safeguard the DPMS sector from being abused by criminals and terrorists, this Guideline aims at providing succinct information on the following -

(a) a general background on ML and TF;
(b) insights to the trade on the ML/TF risks they are facing;
(c) practical guidance to assist DPMS to mitigate the risks; and

[1] Specified transactions include, where appropriate, real estate transactions; management of client money, securities or other assets; management of bank, savings or securities accounts; company formation and management; and buying and selling of business entities.

(d) assistance to DPMS in filing suspicious transaction reports ("STRs").

1.6 DPMS are encouraged to implement the recommended measures in this Guideline among its branches and group members in Hong Kong, as well as those outside Hong Kong.

1.7 This Guideline is advisory in nature and does not constitute legal advice. DPMS are advised to seek independent legal advice where they consider necessary.

2. What Are Money Laundering and Terrorist Financing

Money Laundering

2.1 According to FATF, ML is the processing of crime proceeds to disguise their illegal origin. More specifically, an International Monetary Fund Report[2] describes the process as proceeds generated by crimes such as theft, fraud, corruption, and drug trafficking being made to look as if they are the fruits of honest activities – transformed into seemingly legitimate bank accounts, real estate, or luxury goods.

2.2 In Hong Kong, ML is defined in section 1 of Part 1 of Schedule 1 to AMLO as an act intended to have the effect of making any property -

(a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or

(b) that in whole or in part, directly or indirectly, represents such proceeds,

not to appear to be or so represent such proceeds.

2.3 ML is a criminal offence under the Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP") (Cap. 405) and the Organized and Serious Crimes Ordinance ("OSCO") (Cap. 455). The key provisions of DTROP and OSCO are elaborated in Section 3.

Stages of money laundering

2.4 International typologies suggest that there are three common stages of ML during which there may be numerous transactions made by launderers that could alert a business to possible criminal activity -

(a) **Placement** - the physical disposal of proceeds derived from illegal activity;

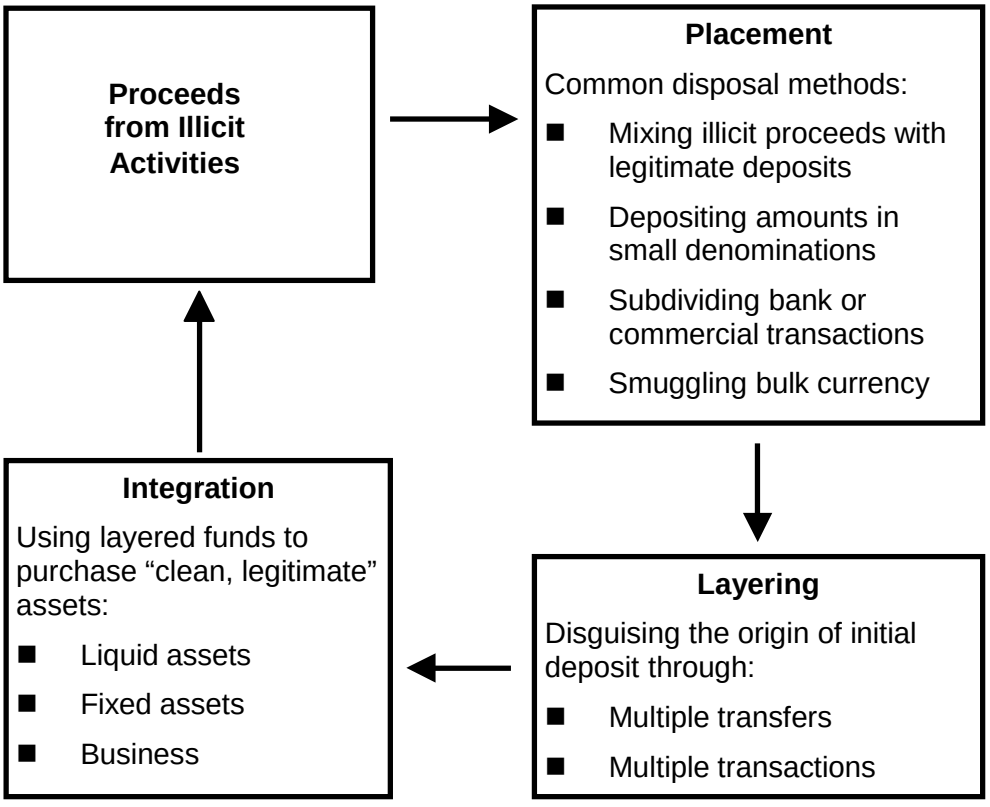
[2] Implementing AML/CFT Measures in the Precious Minerals Sector: Preventing Crime While Increasing Revenue. Available at: https://www.imf.org/en/Publications/TNM/Issues/2016/12/31/Implementing-AML-CFT-Measures-in-the-Precious-Minerals-Sector-Preventing-Crime-While-42441

(b) **Layering** - separating illicit proceeds from their source by creating complex layers of transactions designed to disguise the audit trail and provide anonymity; and

(c) **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes may place the laundered proceeds back into the economy in such a way that they re-enter the financial system or economy appearing to be normal business funds.

2.5 The following chart illustrates a typical cycle of ML –

TYPICAL PROCESS OF MONEY LAUNDERING



Terrorist Financing

2.6 FATF has defined TF as the financing of terrorist acts, and of terrorists and terrorist organisations.

2.7 In Hong Kong, TF is defined in section 1 of Part 1 of Schedule 1 to AMLO as –

(a) the provision or collection, by any means, directly or indirectly, of any property –

(i) with the intention that the property be used; or

(ii) knowing that the property will be used,

in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or

(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

2.8 TF is a criminal offence under the United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO") (Cap. 575). The key provisions of UNATMO are elaborated in Section 3.

Understanding the Risks: Precious Metals and Stones and Money Laundering/Terrorist Financing

2.9 Purchasing precious metals and stones is lucrative to criminals and terrorists as means of ML or TF because of their high value, portability, exchangeability and inherent market characteristics. In the international typology reports published by FATF, the risks of precious metals and stones are recognised.

2.10 In FATF's *Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold*[3] published in July 2015, the gold market is enticing to criminal groups wishing to hide, move or invest their illicit proceeds, since it is highly cash intensive. Gold has high inherent value and worldwide exchangeability; and the anonymous property of gold would make tracking its origins difficult. Crime syndicates typically purchase gold with crime proceeds and resell the gold locally or to another jurisdiction, so that the funds would be further integrated and re-enter the economy. In particular, many transactions involving gold occur anonymously, with little to no record identifying the seller or purchaser. In certain cases, "trade-based ML" ("TBML") occurs whereby proceeds of crime and the value of the gold were moved

[3] Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf

through fictitious trading activities. The gold market has also been identified to pose opportunities for generating proceeds, such as theft, fraud and smuggling activities.

2.11 FATF has also published *Money Laundering and Terrorist Financing Through Trade in Diamonds* in October 2013[4] and discussed the threats and vulnerabilities of the diamond trade in ML/TF. Diamonds are used by criminals for wealth movement, storage and preservation, and as a status symbol; it could also be used as an alternate currency. Diamond trading is vulnerable to ML/TF (including TBML) because of the inherent characteristics, such as high value with low weight/mass, high durability of diamonds, changeability, subjectivity in the evaluation of price, the ease of trade outside the financial system, the significant amounts of the transactions conducted by diamond dealers, and the use of diamonds as alternate currencies by crime syndicates or terrorists. The diamond trade is also where ML activities of placing and layering, as well as trading of illicit diamonds (such as stolen/robbed diamond) could both take place.

2.12 The typology reports aforementioned contain numerous case examples on ML/TF involving precious metals and stones. DPMS in Hong Kong are encouraged to look into these reports to understand the potential risks to their business.

2.13 In *Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report* published in April 2018, a specific section has discussed the risks faced by DPMS[5]. Acknowledging that the reduced use of cash, the domination of lower-value jewellery in the retail market, and the business practices of DPMS in Hong Kong contribute to a relatively lower level of risks locally, DPMS are still strongly advised to maintain vigilance and adopt AML/CFT measures in **Sections 4 to 11** of this Guideline to mitigate risks.

[4] Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

[5] See Chapter 6 of the Report. Available at: www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

3. Understanding the Law on Money Laundering and Terrorist Financing in Hong Kong

3.1 Legislation has been developed in Hong Kong to address the issues associated with the laundering of proceeds of crime and financing of terrorism. The major pieces of AML/CFT legislation include the following –

(a) DTROP;

(b) OSCO;

(c) UNATMO;

(d) AMLO; and

(e) the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629).

These Ordinances cover a wide range of measures on AML/CFT, including the criminalisation of ML/TF, the obligation to make STRs, the preventive measures to be implemented by financial institutions and a number of DNFBPs, and the declaration and disclosure system on the cross-boundary movement of large quantities of cash or instruments concerned. DPMS should note that some measures apply universally and thus they have the statutory obligation to comply with these measures.

Money Laundering Offences

3.2 ML offences are set out in DTROP and OSCO. Sections 25(1) of DTROP and OSCO create the offences of ML, i.e. dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represent the proceeds of drug trafficking or of an indictable offence respectively. These offences carry a maximum sentence of 14 years imprisonment and a maximum fine of $5 million.

Proceeds of an Offence outside Hong Kong

3.3 Proceeds as mentioned in paragraph 3.2 above are not limited to those generated from indictable offences committed in Hong Kong. Section 25(4) of OSCO provides that references to an indictable offence include a reference to conduct, which would constitute an indictable offence if it had occurred in Hong Kong. In other words, it is an offence for a person to deal with the proceeds of crime even if the predicate crime was not committed in Hong Kong, provided that it would constitute an indictable offence if it had occurred in Hong Kong. For proceeds of drug trafficking under section 25 of DTROP, it refers to any proceeds of drug trafficking, whether committed in Hong Kong or elsewhere.

Making Suspicious Transaction Reports

3.4 Sections 25A(1) of DTROP and OSCO impose a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively, or was or is intended to be used in that connection, to disclose the knowledge or suspicion (i.e. make an STR) to an authorised officer[6]. Section 25A(7) makes it an offence for a person failing to file an STR. The offence carries a maximum penalty of three months' imprisonment and a fine of $50,000. The Joint Financial Intelligence Unit ("JFIU")[7] is the designated unit to receive and process STRs. Where a business knows or suspects that any property is the proceeds of crime, it must promptly make a report to JFIU. Details on how to file an STR are set out in **Section 9**.

Protection in law in making suspicious transaction reports

3.5 Sections 25A(3) of DTROP and OSCO provide that an STR made under sections 25A(1) (see paragraph 3.4 above) shall not be treated as a breach of contract or of any enactment restricting disclosure of information, and shall not render the

[6] In DTROP and OSCO, authorized officer means (a) any police officer; (b) any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); and (c) any other person authorized in writing by the Secretary for Justice for the purposes of this Ordinance.

[7] JFIU is jointly operated by the Hong Kong Police Force and the Customs and Excise Department at the Police Headquarters. It was set up in 1989 to receive and analyse STRs, and to disseminate the same to relevant units for investigation.

person making the STR liable in damages for any loss arising out of the report. Therefore businesses need not be concerned about breaching their contracts with or duty of confidentiality owed to customers when making filing STRs under the two Ordinances.

Employees making reports

3.6 Sections 25A(4) of DTROP and OSCO extend the provisions of sections 25A(1) to STRs made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such reports in the same way as it applies to reports to JFIU. This provides defence to employees of business against the risk of prosecution where they have reported knowledge or suspicion of crime proceeds to the person designated by their employers.

"Tipping-off" offence

3.7 A "tipping-off" offence is created under sections 25A(5) of DTROP and OSCO, under which a person commits an offence if knowing or suspecting that an STR has been made, he/she discloses to any other person any matter which is likely to prejudice any investigation that might be carried out following the STR. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and a fine of $500,000.

Protection from Committing Money Laundering Offences

3.8 Sections 25A(2) of DTROP and OSCO provide that if a person who has made an STR does any act in contravention of sections 25(1) and the STR relates to that act, he/she does not commit an offence if –

(a) the STR is made before he/she does that act and the act is done with the consent of an authorised officer (i.e. JFIU); or

(b) the STR is made after the person does the act and the STR is made on the person's own initiative and as soon as it is reasonable for him/her to make it.

Statutory Defence

3.9 It is a defence under sections 25(2) of DTROP and OSCO for a person charged with an ML offence to prove that he/she

intended to disclose such knowledge, suspicion or matter to JFIU, and has a reasonable excuse for his/her failure to make a report in accordance with sections 25A(2) of the two Ordinances.

Terrorist Financing Offences

3.10 TF offences are set out in UNATMO. It implements relevant United Nations ("UN") Security Council Resolutions in preventing and suppressing TF and criminalising the wilful provision or collection of funds for terrorism. The major provisions are as follows –

(a) section 7 prohibits a person from providing or collecting, by any means, directly or indirectly, any property (i) with the intention that the property be used; or (ii) knowing that the property will be used, in whole or in part, to commit terrorist act(s) (whether or not the property is actually so used);

(b) section 8 prohibits a person from (i) making available, by any means, directly or indirectly, any property or financial (or related) services to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate, except under the authority of a licence granted by the Secretary for Security; or (ii) collecting property or soliciting financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate;

(c) section 8A prohibits a person from, except under the authority of a licence granted by the Secretary for Security, directly or indirectly, dealing with any property knowing that, or being reckless as to whether, the property is (i) specified terrorist property; (ii) wholly or jointly owned or controlled, directly or indirectly, by a specified terrorist or terrorist associate; or (iii) held by a person on behalf of, or at the direction of, a specified terrorist or terrorist associate; and

(d) Section 11L prohibits any person from providing or collecting, by any means, directly or indirectly, any property (i) with the intention that the property will be used; or (ii) knowing that the property will be used, in

whole or in part, to finance the travel of any person between states for a specified purpose (whether or not the property is actually so used). A specified purpose means (i) the perpetration, planning or preparation of, or participation in, terrorist act(s) (even if no terrorist act actually occurs); or (ii) the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, terrorist act(s) (even if no terrorist act actually occurs as a result of the training).

3.11 The maximum penalty for breaching sections 7, 8 or 8A is a fine (without cap) and imprisonment for 14 years. The maximum penalty for breaching section 11L is a fine (without cap) and imprisonment for seven years.

Designated Terrorists, Terrorist Associates and Terrorist Property

3.12 Under sections 4 and 5 of UNATMO, where a person or property is designated by a Committee of the UN Security Council or specified by the Court of First Instance as a terrorist/terrorist associate or terrorist property, the details will be specified and published in the Government Gazette and made available at the website of the Security Bureau[8].

Making Suspicious Transaction Reports

3.13 Similar to DTROP and OSCO, section 12(1) of UNATMO makes it a statutory requirement for a person to disclose his knowledge or suspicion that any property is terrorist property (i.e. making an STR) to JFIU. Section 14(5) makes it an offence for a person failing to file an STR, with a maximum penalty of three months' imprisonment and a fine of $50,000. Therefore, where a business knows or suspects that any property is terrorist property, it must promptly make a report to JFIU. Details on how to file a report are set out in **Section 9**.

[8] http://www.sb.gov.hk/eng/special/terrorist/terrorist.htm

Protection in law in making suspicious transaction reports

3.14 Section 12(3) of UNATMO provides that an STR made under section 12(1) (see paragraph 3.13 above) shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, and shall not render the person making the STR liable in damages for any loss arising out of the report. Therefore business need not be concerned about breaching their contracts with or duty of confidentiality owed to customers when making STRs.

Employees making reports

3.15 Section 12(4) of UNATMO provides that section 12 shall have effect in relation to STRs made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such STRs as it has effect in relation to STRs to JFIU. This provides defence to employees of business against the risk of prosecution where they have reported knowledge or suspicion of terrorist property to the person designated by their employers.

"Tipping-off" offence

3.16 A "tipping-off" offence is created under section 12(5) of UNATMO under which a person commits an offence if knowing or suspecting that an STR has been made, he/she discloses to any other person any information or other matter which is likely to prejudice any investigation that might be carried out following the STR. The "tipping-off" offence carries a maximum penalty of three years' imprisonment and a fine without cap.

Protection from Committing Terrorist Financing Offences

3.17 Sections 12(2) and (2A) of UNATMO provides that if a person who has made an STR does any act in contravention of section 7, 8 or 8A(1)(b) or (c) (i.e. elements of (ii) and (iii) in paragraph 3.10(c) above) and the STR relates to that act, he/she does not commit an offence if –

(a) the STR is made before he/she does that act and the act is done with the consent of an authorised officer (i.e. JFIU); or

(b) the STR is made after the person does the act and the STR is made on the person's own initiative and as soon as it is practicable for him/her to make it.

Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)

3.18 AMLO imposes, among other things, obligations to carry out CDD and keep records on financial institutions, and more recently on four DNFBPs, namely legal professionals, accounting professionals, estate agents and TCSPs, when they conduct specified transactions. Under AMLO, a licensing regime has also been established for TCSPs.

3.19 While DPMS are not yet regulated under AMLO, businesses are recommended to implement CDD and record-keeping measures as best practices to identify suspicious transactions and mitigate the risks of ML/TF. More details on the CDD and record-keeping measures are set out in **Sections 6 and 8**.

Declaration and Disclosure of Cash or Instruments Concerned

3.20 The Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629) commenced operation on 16 July 2018. It has established a declaration and disclosure system on the physical cross-boundary transportation of large quantities of currency and bearer negotiable instruments (e.g. bearer cheques, travellers' cheques) ("CBNIs") for preventing terrorists and other criminals from financing their activities or laundering crime proceeds by such means. The system does not restrict the free flow of legitimate capital into and out of Hong Kong.

3.21 Under Cap. 629, any person arriving in Hong Kong at a control point specified in the Ordinance and in possession of a large quantity (i.e. the total value of which is more than $120,000) of CBNIs must make a written declaration to a Customs officer, using the Red Channel under the Red and Green Channel System. Any person who arrives in Hong Kong other than at a control point specified in the Ordinance, or is about to leave Hong Kong, must upon the requirement of a Customs officer disclose whether he/she is in possession of a large quantity of CBNIs. If so, he/she must make a written declaration on the CBNIs.

3.22 For cargoes, an advance electronic declaration must be made for the import or export of a large quantity of CBNIs in a cargo consignment through the designated system of the Customs and Excise Department (www.customs.gov.hk). The declaration requirement does not apply to cargoes in transit, air

transhipment cargoes and mails.

3.23 The maximum penalty for breaching the declaration or disclosure requirements is a fine of $500,000 and two years of imprisonment.

4. Basic Policies and Measures to Combat Money Laundering and Terrorist Financing

4.1 Generally, DPMS are advised to have in place a set of policies and measures on AML/CFT as follows, in compliance with the essential FATF standards –

(a) taking a risk-based approach (see **Section 5**);
(b) applying CDD (see **Section 6**);
(c) continuous monitoring of customers (see **Section 7**);
(d) record keeping (see **Section 8**);
(e) making STRs (see **Section 9**);
(f) internal controls (see **Section 10**); and
(g) staff education and training (see **Section 11**).

4.2 It is advisable for DPMS to issue a clear statement of policies in relation to AML/CFT. This statement should be communicated in writing to all management and relevant staff whether in branches, departments, or subsidiaries, and should be reviewed on a regular basis.

4.3 Where possible, instruction manuals should be prepared to set out the businesses' procedures for the measures in paragraph 4.1 above.

5. Taking a Risk-based Approach

5.1 DPMS in Hong Kong have diverse activities, modes of operation and clientele. Risks would vary according to the activities undertaken by DPMS. DPMS should take appropriate steps to identify, asses and understand their ML/TF risks, and take proportionate actions to mitigate the risks identified, i.e. taking a "risk-based" approach ("RBA").

5.2 Risk assessment is central to RBA. While there is neither a universally applicable set of risk factors nor a single methodology to apply risk factors in determining the ML/TF risk rating of customers, the following factors are commonly taken into consideration in risk assessment-

(a) **customer risk** (e.g. significant use of cash in transactions; payment made by or delivery of products to third parties; the customer is a politically exposed person ("PEP") (more details in **Section 6**);

(b) **country/geographic risk** (e.g. the customer resides in or is connected with high-risk jurisdictions, such as jurisdictions identified by FATF as having deficient systems to prevent ML/TF or subject to sanctions by the UN);

(c) **product/service risk** (e.g. the customer buys high-value and easily portable jewellery; opens gold accounts for transferring gold to destinations worldwide); and

(d) **delivery channel risk** (e.g. non face-to-face transactions).

5.3 DPMS may have a network of business counterparties (e.g. foreign suppliers or agents of distribution). The same framework of risk assessment above may apply to such counterparties.

5.4 The general principle of an RBA is that where customers are assessed to be of higher ML/TF risks, DPMS should take enhanced measures to manage and mitigate those risks.

6. Applying Customer Due Diligence

6.1 Knowing your customer is a key facet of RBA and enables you to recognise suspicious circumstances or abnormality in the transaction(s) of the customer. CDD is intended to enable a business to form a reasonable belief that it knows the true identity of the customer or the beneficial owner[9] and, with an appropriate degree of confidence, knows the type of business and transactions the customer is likely to undertake. By carrying out CDD, DPMS may use the CDD information as an important basis for recognising whether there are grounds for suspicion of ML/TF activities.

Customer Due Diligence Measures

6.2 CDD is not necessary in every single transaction. FATF's standards require that DPMS undertake CDD **when they are involved in any cash transaction with a customer of or above USD/EUR 15,000 (around HK$120,000)**. Drawing reference from AMLO, the recommended CDD measures include –

(a) identifying the customer and verifying the customer's identity based on documents, data or information from reliable and independent sources (e.g. Hong Kong identity card, passport, companies registration);

(b) where there is a beneficial owner in relation to the customer, identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity;

(c) obtaining information on the purpose and intended nature of the business relationship (if any) to be established with the DPMS; and

(d) if a person purports to act on behalf of the customer –

(i) identifying the person and taking reasonable measures to verify the person's identity based on

[9] According to FATF, "beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement (e.g. a company). A definition of "beneficial owner" is provided in section 1 of Schedule 2 to AMLO.

documents, data or information from reliable and independent sources; and

(ii) verifying the person's authority to act on behalf of the customer.

6.3 In high-risk situations including but not limited to the following, enhanced due diligence measures should be adopted –

(a) customer not physically present for identification purposes;

(b) customer or the beneficial owner being a PEP (see **paragraphs 6.6 to 6.10 below**); and

(c) customer from or transaction connected with a jurisdiction that does not adopt or insufficiently adopts the FATF Recommendations.

6.4 Enhanced due diligence measures may include –

(a) for the situation in paragraph 6.3(a) above, further verifying the customer's identity based on further available documents, data or information; taking supplementary measures to verify information relating to the customer; or ensuring that the payment is made through regulated financial channels (e.g. banks);

(b) for situations in paragraph 6.3(b) or (c) above –

(i) obtaining approval from the senior management of the DPMS; and

(ii) taking reasonable measures to understand the customer's or the beneficial owner's source of wealth and the source of funds that will be/are involved in the transaction.

6.5 Simplified due diligence may be conducted for customers in lower-risk situations, i.e. without suspicion on ML/TF and doubt on the veracity of information used to identify the customer's identity, such as the Government, public bodies, financial institutions and listed companies. In conducting simplified due diligence, measures in paragraphs 6.2(a), (c) and (d) above should suffice.

Politically Exposed Persons

6.6 As paragraphs 6.2 and 6.3 above suggest, where the customer or the beneficial owner is a PEP and engages in a cash transaction of on above HK$120,000, DPMS are advised to carry out enhanced due diligence measures. Under AMLO, PEP is defined as –

(a) an individual who is or has been entrusted with a prominent public function in a place **outside** the People's Republic of China –

(i) including a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;

(ii) but not including a middle-ranking or more junior official of any of the categories mentioned in subparagraph 6.6(a)(i) above;

(b) a spouse, a partner, a child or a parent of an individual covered by paragraph 6.6(a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual covered by paragraph 6.6(a).

6.7 A close associate is defined as –

(a) an individual who has close business relations with a person covered by paragraph 6.6(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person covered by paragraph 6.6(a) above is also a beneficial owner; or

(b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person covered by paragraph 6.6(a) above.

6.8 DPMS are advised to be vigilant and gather sufficient information from a customer, and check publicly available information to establish as far as possible whether the customer is a PEP. If an individual is known to be a PEP, DPMS should perform enhanced due diligence measures (see paragraphs 6.3

and 6.4 above).

6.9 An RBA may be adopted for identifying PEPs and focus may be put on persons from countries or jurisdictions that have a higher prevalence of corruption. Risk factors that DPMS should consider in handling a transaction with a PEP may include the following –

(a) any particular concern over the country or jurisdiction where the PEP is from, taking into account the PEP's position;

(b) any unexplained source of wealth or income (i.e. value of assets owned not in line with the PEP's income level);

(c) any source of wealth described as commission earned on government contracts;

(d) any request by the PEP to associate any form of secrecy with a transaction; and

(e) any use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

Domestic Politically Exposed Persons and Office-bearers of International Organisations

6.10 While PEP is defined under AMLO to include individuals entrusted with a prominent public function in a place outside the People's Republic of China[10], domestic PEPs and persons who are or have been entrusted with a prominent function by international organisations [11] may also present, by their positions, a high risk situation. DPMS should therefore assess the risk and determine whether to apply enhanced due diligence measures.

[10] Including the Mainland, Hong Kong Special Administrative Region, Macao Special Administrative Region and Taiwan.

[11] Persons who are or have been entrusted with a prominent function by international organisations refer to members of senior management, i.e. directors, deputy directors and members of the board or equivalent in an international organisation.

7. Ongoing Monitoring of Customers

7.1 DPMS may have customers with whom they have established a long-standing business relationship. For such customers, effective continuous monitoring helps DPMS understand their customers' activities, update the knowledge of their customers and detect unusual or suspicious activities.

7.2 A DPMS should continuously monitor the business relationship with a customer with whom it has established relationship by –

(a) reviewing from time to time documents, data and information relating to the customer to ensure that they are up-to-date and relevant;

(b) conducting appropriate scrutiny of transactions with the customer to ensure that they are consistent with the DPMS' knowledge of the customer and the customer's business, risk profile and source of funds; and

(c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose, and examining the background and purposes of such transactions and recording the findings.

7.3 Possible features a DPMS should consider monitoring include:

(a) the nature and type of transactions (e.g. abnormal amounts or frequency);

(b) the nature of a series of transactions (e.g. a number of small value transactions);

(c) the amount of any transactions, paying particular attention to particularly substantial transactions;

(d) the geographical origin/destination of a payment or receipt; and

(e) the customer's normal activities or turnover.

8. Record Keeping

8.1 Record keeping is an integral part of AML/CFT measures as it provides an audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds.

8.2 Record keeping helps investigating authorities establish the profile of a suspect, traces a criminal's or terrorist's property or funds, and assists the court to examine all relevant transactions to assess whether the property or funds are the proceeds of or relate to criminal offences or terrorist activities.

8.3 DPMS should take steps to ensure that records of their customers with whom they have carried out transactions of HK$120,000 or above in cash are kept. The records that should be kept include –

(a) data and information obtained in connection with the transactions;

(b) where CDD has been conducted, the data and information obtained in the course of identifying and verifying the identity of the customer or any beneficial owner; and

(c) files relating to a customer's account (if any) and business correspondence with the customer and any beneficial owner of the customer.

8.4 FATF standards require that the records of transactions be kept for at least **five** years after the transaction. For records on CDD, a customer's account and business correspondence with the customer, records should be kept throughout the continuance of the business relationship with the customer and for a period of at least **five** years beginning on the date on which the business relationship ends[12]. The records could be either in hardcopy or computerised.

[12] For many transactions handled by DPMS, the business relationship is one-off and ends at the time when the transaction is completed.

9. Making Suspicious Transaction Reports

Legal Obligation

9.1 Paragraphs 3.4 and 3.13 above explain the statutory requirement on **every person** to file STRs related to ML and TF to JFIU. This section elaborates the practical aspects of filing STRs.

The Joint Financial Intelligence Unit

9.2 The Hong Kong Police Force and the Hong Kong Customs and Excise Department jointly run JFIU. JFIU manages the STR regime governed by DTROP, OSCO and UNATMO. It is the sole agency in Hong Kong to receive, analyse, and disseminate STRs to agencies concerned as appropriate.

9.3 JFIU also offers practical guidance and assistance to the financial and DNFBP sectors on AML/CFT.

Identification of Suspicious Transactions

9.4 While it is not possible to list out all possible scenarios which may constitute suspicious transactions, JFIU's **SAFE approach** – **S**creen, **A**sk, **F**ind and **E**valuate (see https://www.jfiu.gov.hk/en/str.html#how) – provides a useful method for identifying a suspicious transaction. Specific to the DPMS sector, a number of commonly seen "red flag" scenarios are listed at **Annex** for easy reference. They are by no means exhaustive, and DPMS should examine individual scenarios they encounter to determine whether filing STRs is warranted.

9.5 For ML, it is not necessary to ascertain the underlying predicate crime for STRs to be filed.

9.6 As regards TF, DPMS should check their potential customers against the list of designated terrorists and terrorist associates as well as persons subject to UN sanctions available at JFIU's website (https://www.jfiu.gov.hk) to ascertain whether any customer may be related to a terrorist, terrorist associate or parties involved in the proliferation of weapons of mass destruction.

9.7 DPMS are encouraged to visit JFIU's website from time to time (http://www.jfiu.gov.hk) which provides typologies, information on the latest ML/TF trends, lists of designated terrorist/terrorist associates and persons subject to UN sanctions and other AML/CFT matters of interest to the sector.

Corporate Responsibility

9.8 It is a good practice for DPMS to appoint a designated officer (e.g. a compliance officer) who is to be responsible for receiving and assessing internal STRs filed by frontline employees.

9.9 The designated officer should keep a register of all STRs made by employees and all STRs made to JFIU. The designated officer should provide employees with a written acknowledgement of STRs made to him/her, which will form part of the evidence that the STRs were made in compliance with the internal procedures.

9.10 Where an employee of a DPMS **knows** that the property in whole or in part directly or indirectly represents/was used/ intended to be used in connection with proceeds of crime or terrorist property, under no circumstances should the employee conduct any transaction with the customer. An STR should be promptly filed with the designated officer who, in turn, should immediately forward the STR to JFIU.

9.11 Where an employee of a DPMS **suspects** that the property in whole or in part directly or indirectly represents/was used/ intended to be used in connection with proceeds of crime or terrorist property, this information must also be promptly reported to the designated officer. If the circumstances remain to be suspicious after assessment, the designated officer should forward the STR to JFIU.

9.12 In any case, the designated officer's findings and supporting reasons should be documented, especially for a decision not to report to JFIU. The reporting employee should also be advised, on a confidential basis, on how his/her report has been handled.

9.13 The fact that an STR may already have been filed with JFIU in relation to previous transactions of a customer **should not preclude the making of a fresh STR if there are new suspicions**.

9.14 In reporting to JFIU, the designated officer should ensure that all relevant details are provided in an STR and cooperate fully with JFIU for the purpose of investigation.

9.15 DPMS should take steps to ensure that all employees involved directly in the purchase or sale of precious metals/stones are aware of these procedures and that it is a criminal offence to fail to report either knowledge or suspicion of proceeds of crime or terrorist property.

How to Report Suspicious Transactions

9.16 DPMS should make STRs to JFIU as soon as it is reasonable for them to do so. The reporting proforma is available at JFIU's website (https://www.jfiu.gov.hk).

9.17 JFIU has launched a web-based platform to facilitate e-reporting and processing of STRs, called the Suspicious Transaction Report and Management System ("STREAMS"). DPMS who intend to file STRs at this platform should apply to JFIU. The application form can be downloaded from JFIU's website (https://www.jfiu.gov.hk/en/str.html#how).

9.18 Following receipt of an STR and analysis by JFIU, the information may be referred to an appropriate local/overseas law enforcement agency or financial intelligence units for the prevention or detection of crime.

Post-reporting Precaution

9.19 DPMS are reminded that the law prohibited "tipping-off" of their customers upon the filing of an STR (see paragraphs 3.7 and 3.16 above). Where it is known or suspected that an STR has been filed with JFIU and it becomes necessary to make further enquiries of the customer, great care must be taken to ensure that the customer does not become aware that his/her name or activities have been brought to the attention of JFIU.

Confidentiality of Identity

9.20 All STRs are dealt with in strict confidence as required by the relevant provisions of the three Ordinances (DTROP, OSCO and UNATMO). Sections 26 of DTROP and OSCO and section 12 of UNATMO impose strict restrictions on revealing STR information. The confidentiality of the STR reporting

entities' identity is considered to be of paramount importance to maintain the integrity of STR regime as well as the mutual trust between JFIU and the reporting entities.

10. Internal Controls

10.1 The senior management of a DPMS should be fully committed to establishing appropriate policies and procedures for the prevention of ML/TF and ensuring their effectiveness. Explicit responsibility should be allocated within a business for this purpose.

Compliance Officer

10.2 A DPMS should appoint a compliance officer as a central reference point for dealing with AML/CFT matters. The compliance officer should play an active role in the receiving and assessing STRs (see also paragraphs 9.8 to 9.15 above). This should involve regular reviews of reports of large or irregular transactions generated by the business' management information system as well as *ad hoc* reports made by frontline staff. Depending on the business' organisational structure, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

10.3 The compliance officer should have the responsibility of checking, on an ongoing basis, that the business has policies and procedures to ensure compliance with legal requirements and of testing such compliance.

10.4 It follows from this that a DPMS should ensure that the compliance officer is of a sufficient status within the organisation, and has adequate resources to enable him/her to perform his/her functions.

Internal Audit

10.5 Internal audit has an important role in independently evaluating, on a periodic basis, a business' policies and procedures on AML/CFT. This should include checking the effectiveness of the compliance officer's functions, the adequacy of the management information system, reports of large or irregular transactions, and the quality of reporting of suspicious transactions. The level of awareness of frontline staff of their responsibilities in relation to the prevention of ML should also be reviewed. The internal audit section should have sufficient expertise and resources to enable it to carry out its responsibilities.

10.6 DPMS should instruct their internal audit/inspection units to verify, on a regular basis, compliance with policies, procedures, and controls against ML and TF.

11. Staff Education and Training

11.1 Staff should be aware of their own personal legal obligations under DTROP, OSCO and UNATMO and that they can be personally held liable for failure to file STRs to JFIU. They should co-operate fully with the law enforcement agencies and promptly report suspicious transactions. They should be advised to report suspicious transactions to JFIU or their companies' compliance officers (if designated) even if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

11.2 It is therefore imperative for DPMS to introduce comprehensive measures to ensure that their staff are fully aware of their responsibilities.

11.3 DPMS should provide proper AML/CFT training to their local as well as staff outside Hong Kong. The timing and content of training packages for various levels of staff will need to be adapted by individual businesses for their own needs. Meanwhile, training covering the following elements is recommended -

(a) New Employees

New employees, who will be dealing with customers or their transactions, irrespective of the level of seniority, should have a general understanding of the background about ML and TF, the consequent need to be able to identify suspicious transactions and make STRs to the appropriate designated officer within the business or JFIU, the "red flags" for STRs, the offence of "tipping-off", and the CDD and record keeping procedures adopted by the business. They should be familiar with the legal requirements and their personal statutory obligation to file STRs.

(b) Frontline Staff

Members of staff who are dealing directly with members of the public are the first point of contact with potential money launderers. Their efforts are therefore vital to the business' strategy in the fight against ML and TF. They should be familiar with their legal responsibilities, the business' system for filing STRs, conducting CDD and

keeping records. In particular, frontline staff should receive adequate training on the “red flags” of suspicious transactions and the need for extra vigilance in such circumstances.

(c) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of AML/CFT procedures should be provided to those with the responsibility of supervising or managing staff. This should include information on the relevant offences and penalties under DTROP, OSCO and UNATMO, etc.

(d) On-going Training

It will also be necessary to make arrangements for refresher training regularly. In this connection, seminars are organised by the Government from time to time for the DPMS sector on AML/CFT. Employees of DPMS should be encouraged to join.

List of Acronyms and Abbreviations

AML	anti-money laundering
AMLO	Anti-money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
CBNI	currency and bearer negotiable instrument
CDD	customer due diligence
CFT	counter-financing of terrorism
DNFBP	designated non-financial businesses and professions
DPMS	dealers in precious metals and stones
DTROPO	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
FATF	the Financial Action Task Force
JFIU	the Joint Financial Intelligence Unit
ML	money laundering
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP	politically exposed person
RBA	risk-based approach
STR	suspicious transaction report
TBML	trade-based money laundering
TCSPs	trust or company service providers
TF	terrorist financing
UN	the United Nations
UNATMO	the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)

Annex - Examples of "Red Flag" Scenarios

*For **retail market** –*

(a) Incommensurate background of buyer (e.g. profession and age of buyer not commensurate with amount of transactions and type of precious stones and metals involved);

(b) Large amount transactions conducted in cash but not in other popular and safe methods of payment (e.g. credit card);

(c) Unusual payment method (payment by negotiable instruments in bearer form, e.g. travellers cheques and cashier orders where the fund provider cannot be traced);

(d) Unusual buying behaviour/pattern (e.g. repeated purchases of luxury products without apparent reasons);

(e) Unusual behaviour of the person(s) conducting the transactions (e.g. unusual nervousness); and

(f) Request for over/under-invoicing of purchases.

*For **wholesale market** –*

(a) Incommensurate background of buyer/seller (e.g. profession and age of buyer/seller not commensurate with amount of transaction and type of precious metals and stones involved);

(b) Unknown business background of buyer/seller;

(c) Transactions conducted by third party not related to the buyer/seller;

(d) Transactions conducted by shell company/offshore company;

(e) Unknown source of precious metals/stones;

(f) Unknown purpose of transactions;

(g) Buyer/seller apparently not having reasonable expertise/experience in the precious metals/stones sector;

(h) Abnormally low/high pricing or with substantial discount/premium in order to speed up transactions;

(i) Large amount of transactions from an unfamiliar dealer;

(j) Request for over/under-invoicing of purchases;

(k) Unusual payment method (payment by third party/payment by negotiable instruments in bearer form, e.g. travellers cheques and cashier orders where the fund provider cannot be traced);

(l) Buyer/seller refusing to use other means of payment other than cash, while cash may be in foreign currencies (or in different foreign currencies), without apparent reasons; and

(m) Unusual business pattern (e.g. business transactions of a particular dealer are rather frequent when compared to the trading history of other dealers/a sudden increase in the trading volume without apparent reasons).