CODE OF PRACTICE: ANTI-MONEY LAUNDERING MEASURES FOR PRECIOUS STONES AND PRECIOUS METALS DEALERS TO COMBAT SCAM-RELATED MONEY LAUNDERING CASES

1. Purpose

1.1. This Code of Practice ("**CoP**") is issued by the Registrar of Regulated Dealers under section 35(1) of the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019 ("**PSPM Act**").

1.2. This CoP sets out the anti-money laundering ("**AML**") measures that Precious Stones and Precious Metals Dealers ("**PSMDs**") should incorporate into their business processes to combat scam-related money laundering ("**ML**") cases.

1.3. The objectives of this CoP are to:

(a) highlight scam typologies involving the use of precious metals, jewellery and luxury watches as a money laundering vehicle;
(b) equip PSMDs with knowledge on red flags in customer transactions; and
(c) establish clear response measures when suspicious activities are detected.

2. Scope and Application

2.1. This CoP applies to all PSMDs registered under section 7 of the PSPM Act conducting sales to or purchases from customers or intermediaries, whether in-person or online.

3. Scam Typologies Relevant to PSMDs

<u>Money Mules in Scam Operations</u>

3.1 Online scams are predominantly carried out by perpetrators based overseas. They recruit money mules through online networks (e.g., messaging platforms) and exploit these physical networks in Singapore to launder their proceeds and subsequently move them overseas. In some cases, mules were asked to purchase precious metals, jewellery and luxury watches from local retailers using cash, bank transfer, PayNow, Cashier's Order or credit card.

3.2 Money mules may exhibit suspicious behaviours when purchasing the high-value items, such as appearing anxious or staying on phone calls throughout the process. The nature of their purchases may be inconsistent with their stated intentions. For example, they may make large and hurried purchases without regard to value, quantity or price. In addition, individuals may be observed waiting outside the premises while the money mule conducts transactions using bank accounts or credit cards that do not belong to him/her.

Scam Victims Manipulated into Making Purchases

3.3 Scammers may also instruct scam victims to purchase precious metals, jewellery, or luxury watches. These are often victims of Government Officials Impersonation Scams and Investment Scams. In cases observed by the Police, victims were typically convinced that they were assisting in legitimate investigations or transactions following unsolicited calls from individuals impersonating representatives from financial institutions, government agencies, or other organisations.

3.4 Like money mules, scam victims may appear anxious, distressed, or remain engaged with their phones (e.g., taking calls and checking messages) during transactions. They typically make large purchases of precious metals, jewellery or luxury watches without any apparent justification. In some cases, victims may also visit the same retailers on consecutive days to make such purchases.

3.5 Scam victims are typically manipulated through social engineering and manipulation tactics. They may insist that their purchases are legitimate and willingly provide their personal identification information, as they genuinely believe that they are complying with official procedures. They would usually discover the fraud after they have surrendered the valuables and the scammers become uncontactable.

3.6 PSMDs should pay **particular attention** to single or multiple purchases of precious metals, jewellery, or other luxury watches **above S$20,000**, especially when made by **elderly customers**.

4. Scam Red Flags

4.1 PSMDs should look out for typical red flags indicating that customers may be money mules or scam victims.

Both Mules and Victims

(a) Customers making unusually large purchases (e.g., above S$20,000) for gold bars, jewellery, luxury watches, etc.;
(b) Customers appearing to be in a hurry to complete the transactions;
(c) Customers seeking to complete transactions without due consideration of their purchases (e.g., price, value, design) or normal browsing behaviour;
(d) Customers avoiding or refusing to provide information on the reason for the purchases, or providing explanations that sound scripted or unnatural;
(e) Customers getting agitated when probed about their large purchases;
(f) Customers providing explanation(s) for the purchases which are inconsistent with the nature of the purchases, when compared against similar purchases or customers;
(g) Customers requesting to split payment using multiple cards without apparent reason;
(h) Customers making repeated high-value purchases within days;

Mule-Specific

(i) Customers attempting to resell substantial quantities of gold;
(j) Customers being reluctant or unable to verify identity on payment modes (e.g., credit cards) with their identification documents;
(k) Customers providing payment details that do not match their known customer profile;
(l) Customers cancelling transactions when they are almost complete;

Victim-Specific

(m) Customers appearing distressed or receiving phone calls while making purchases; and
(n) Customers displaying unfamiliarity with products they are purchasing (e.g., not knowing gold purity, weights, or market prices).

5. Frontline Response Measures

5.1 PSMDs should apply the **A.C.T.** framework at paragraph 5.2 when encountering customers making purchases under the following circumstances, regardless of payment mode:

(a) Single transaction of more than S$20,000; or
(b) Multiple transactions below S$20,000 that collectively exceed S$20,000, whether conducted on the same day or over a few days.

5.2 The **A.C.T.** framework involves the following steps:

	Description	**Possible Questions/Actions**
A	**Add** immediate intervention by asking the customer for reasons behind the purchase.	a. Who are these items for? b. Did anyone instruct you to purchase these items?
C	**Check** for the customer's behaviour using the various anti-scam information at Annex A.	a. Share Annex A with the customer and highlight the prevalent scam tactics.
T	**Tell** the customer that he/she should call the ScamShield Helpline at 1799 or 999 if he/she is under instructions to make the purchases.	a. Emphasise that Singapore government officials will never **(i)** ask you to transfer or hand over valuables such as money, gold or luxury watches, or **(ii)** transfer your call to the Police or any other government officials, including Monetary Authority of Singapore and Ministry of Law. b. Encourage the customer to **(i)** check for scam signs with official sources, and **(ii)** tell the authorities, family, and friends about scams.

5.3 If any red flags described in paragraph 4 are identified when carrying out **A.C.T.**, PSMDs should have reason to believe that the customers/ transactions present a high risk of ML/TF/PF, and the following steps should be taken:

(a) Conduct enhanced customer due diligence in accordance with the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Regulations 2019;

(b) Seek additional verification of the purchase from the customer's family member by phone;

(c) Request the customer to contact the ScamShield Helpline at 1799 or 999 for assistance;

(d) Provide the customer with anti-scam educational materials or information about common scam tactics, such as resources from Annex A, the ScamShield website (www.scamshield.gov.sg) or Police news releases (SPF | News);

(e) Escalate the matter to the supervisor or senior management and document the customer's behaviour and the basis for proceeding with the transaction;

(f) If the customer proceeds despite warnings and red flags are present, consider calling the police at 999 for urgent assistance; and

(g) File a Suspicious Transaction Report ("**STR**").

5.4 For online sales, in-person collection should be required for purchases above S$20,000. PSMDs should then apply **A.C.T**.

5.5 If **A.C.T.** has not been applied (e.g., for transaction amount S$20,000 and below) but there is suspicion that a customer may be a money mule or a scam victim as described in paragraph 3 or exhibits any red flags described in paragraph 4 of the CoP, the transaction should be treated as high-risk and conduct the mitigation measures listed at paragraph 5.3(a) to 5.3(g).

5.6 PSMDs can use the document at Annex B as a step-by-step guide when engaging customers purchasing above S$20,000 or when customers exhibit suspicious behaviour as described in paragraph 4. Annex B has been made available both as an online form or printable format.

6. Record-Keeping

6.1 PSMDs should maintain appropriate records of the transactions involving purchases above S$20,000 or when the customer exhibits suspicious behaviour as described in paragraph 4. This will help relevant authorities understand the circumstances and the measures taken by the PSMDs.

6.2 Such records also support PSMDs' internal review and continuous improvement of anti-scam controls, enabling PSMDs to enhance their operational effectiveness in combating scams.

7. Additional Internal Measures

7.1 PSMDs may implement additional internal anti-scam measures beyond those specified in this CoP, including enhanced monitoring systems, specialised staff training programmes, or customer communication protocols such as issuing anti-scam advisories or requiring customer declarations that they are not being scammed or acting under instructions, that align with their business model and operational requirements.

Annex A

SCAM TACTICS

Government officials will **never** ask you to transfer or hand over valuables such as money, luxury watches, and gold.
Government officials will **never** transfer phone calls to other government agencies.

IMPERSONATION:
Scammers pose as bank staff, insurance agents, telco staff, or government officials (e.g., from MAS, SPF, Ministry of Law, China Police, Malaysian Police).

UNAUTHORISED TRANSACTIONS:
Unauthorised transactions: Claims of suspicious activities in bank account(s) or on bank cards.

FAKE INSURANCE POLICIES / MOBILE PLANS / CREDIT CARD REGISTRATIONS:
Request for payment for premiums or fees for insurance policies, mobile plans, or credit cards allegedly registered under victims' name. Threats of arrest or police investigation if not cooperative.

ALLEGATIONS OF INVOLVEMENT IN CRIME:
Accuse victims of being involved in criminal activities (e.g., money laundering).

PHONECALLS:
Unsolicited calls from unknown parties. Citing of personal details such as full name and NRIC.

FAKE OFFICIALS:
Phone call transferred to or call back from government officials.

ACCUSATIONS:
Involvement with crime, money laundering activities and threats of legal action, arrest, or asset freezing.

HAND OVER OF CASH OR VALUABLES:
Coerced to transfer money or buy valuables (e.g. gold, luxury watches), to be handed to "government officials" to prove innocence, for investigation, or for safekeeping.

WHEN UNSURE:
CALL SCAMSHIELD HELPLINE AT
1799 OR **999** FOR ASSISTANCE

Scam Alert Questionnarie

Annex B-1

FormSG Questionnaire: Scam Alert Questionnaire | FormSG

https://go.gov.sg/cop-proforma

Annex B-2

Scam Alert Questionnaire

Instructions
PSMDs should record transactions with customers exhibiting the red flags in paragraph 4 of the Code of Practice ("CoP") and steps in paragraph 5 of the CoP should be taken. A completed copy of this form will be sent to the email in question 3, upon successful submission.

Please note that the red flags highlighted are not exhaustive and may not cover every possible scenario. We encourage you to remain vigilant and keep an eye out for any additional red flags that may arise beyond those listed.

If the customer proceeds despite warnings and red flags are present, consider calling the police at 999 for assistance.

1. Date of transaction

_____

2. Name of officer
   Frontline staff who is dealing with the customer

_____

3. Invoice/Transaction Ref Number (if any) (optional)

_____

4. Transaction Amount (S$)

_____

5. Description of transaction
   (e.g. sale of gold bullion)

_____

6. Does the customer exhibit any red flag behaviours before applying A.C.T.?
   for e.g.
   (a) Customers appearing distressed or receiving phone calls while making purchases;
   (b) Customers seeking to complete transactions without due consideration of their purchases (e.g., price, value, design) or normal browsing behaviour; or
   (c) Customers seeking to complete transactions without due consideration of their purchases (e.g., price, value, design) or normal browsing behaviour

No	Yes

7. Has A.C.T. been applied?
   A – Add immediate intervention by asking the customer for reasons behind the purchase.
   C – Check for the customer's behaviour using the various anti-scam information at Annex A.
   T – Tell the customer that he/she should call the ScamShield Helpline at 1799 or 999 if he/she is under instructions to make the purchases.

No	Yes

Please keep a look out for potential red flags, as depicted below.

8. TRANSACTION BEHAVIOUR
   (a) Customers making unusually large purchases (e.g., above $20,000) for gold bars, jewellery, luxury watches, etc.
   (b) Customers appearing to be in a hurry to complete the transactions
   (c) Customers seeking to complete transactions without due consideration of their purchases (e.g., price, value, design) or normal browsing behaviour
   (d) Customers making repeated high-value purchases within days
   (e) Customers attempting to resell substantial quantities of gold
   (f) Customers displaying unfamiliarity with products they are purchasing (e.g., not knowing gold purity, weights, or market prices)

☐ Yes, customer is exhibiting one or more of the above

☐ No

9. CUSTOMER DEMEANOUR
   (a) Customers getting agitated when probed about their large purchases
   (b) Customers appearing distressed or receiving phone calls while making purchases

☐ Yes, customer is exhibiting one or more of the above

☐ No

10. PURCHASE JUSTIFICATION
   (a) Customers refusing to provide information on the reason for the purchases, or providing explanations that sound scripted or unnatural
   (b) Customers providing explanation(s) for the purchases which are inconsistent with the nature of the purchases, when compared against similar purchases or customers

☐ Yes, customer is exhibiting one or more of the above

☐ No

11. PAYMENT BEHAVIOUR
   (a) Customers requesting to split payment using multiple cards without apparent reason
   (b) Customers being reluctant or unable to verify identity on payment modes (e.g., credit cards) with their identification documents
   (c) Customers providing payment details that do not match their known customer profile
   (d) Customers cancelling transactions when they are almost complete

☐ Yes, customer is exhibiting one or more of the above

☐ No

12. Please describe any other behaviours or items that you wish to highlight arising from this transaction. (optional)

13. Please indicate by ticking the appropriate boxes below, if the following mitigation measures were undertaken.

- ☐ Conduct enhanced customer due diligence in accordance with the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Regulations 2019
- ☐ Seek additional verification of the purchase from the customer's family member by phone
- ☐ Request the customer to contact the ScamShield Helpline at 1799 or 999 for assistance
- ☐ Provide the customer with anti-scam educational materials or information about common scam tactics, such as resources from Annex A, the ScamShield website or Police news releases
- ☐ Escalate the matter to the supervisor or senior management and document the customer's behaviour and the basis for proceeding with the transaction;
- ☐ If the customer proceeds despite warnings and red flags are present, consider calling the police at 999 for urgent assistance
- ☐ File a Suspicious Transaction Report ("**STR**")
- ☐ None of the above

14. If the response to the preceding question is "None of the above" or not all the four mitigation measures were undertaken, please indicate the reason(s) as to why the mitigation measures were not carried out.
    Please indicate "N.A." if an option other than "None of the above" was chosen in the preceding question.
