RED FLAG INDICATORS FOR PRECIOUS STONES AND METALS DEALERS (PSMDs)

If a PSMD, in the course of business, knows or has reasonable grounds to suspect that any property is linked to drug dealing or criminal conduct (or generically refer to as "crime"), he is required to disclose his knowledge or suspicion to the Suspicious Transaction Reporting Office (STRO). Please refer to STRO's website[1] on how to lodge a Suspicious Transaction Report (STR) with STRO.

The list of indicators below serves only as an aid for PSMDs in identifying some of the circumstances that could be suspicious in nature or indicative of money being laundered (ML) or used for terrorism financing (TF) purposes. While each individual indicator may be insufficient to suggest that ML/TF is taking place, a combination of such indicators may be indicative of a suspicious transaction. This list is not exhaustive and may be updated due to changing circumstances and new ML/TF methods. PSMDs are to refer to STRO's website for the latest list of red flags.

Red Flag Indicators: Customers[2]	**Red Flag Indicators: Suppliers**
Transaction Patterns	
i) Transactions that are not consistent with the usual profile of a customer: (a) Transactions that appear to be beyond the means of the customer based on his/her stated or known occupation or income; (b) Transactions that appear to be more than the usual amount or quantity for a typical customer of the business; or (c) Transaction purposes that are not in line with the known or expected operations of the business. ii) Large amounts of cash, traveller's cheques, cashier's cheques or trade-in PSPM involved in the transactions.	i) Transactions that are not consistent with the usual profile of a supplier: (a) Over or under-invoicing, structured, complex, or multiple invoice requests, and high-dollar shipments that are over or underinsured; or (b) Transactions which are excessive, given the amount or quality, or potential profit from the sale of PSPM; or (c) Consignment size or type of PSPM shipped appears inconsistent with the capacity of the exporter or importer. For example, the shipment or transshipment does not make economic sense.

[1] The website address as at 23 March 2021: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

[2] A "customer" in this context means a person with whom a regulated dealer enters into or intends to enter into a transaction. Precious stones, precious metals and precious products are collectively referred to as "PSPM" in the red flag indicators.

iii) Large or frequent transactions that are made in a foreign currency. iv) Transactions in which third parties are involved, either as payers or recipients of payment or PSPM, without apparent legitimate business purpose. For example: (a) Payments received from a third party, who is not the owner of the funds, without legitimate business purpose; (b) Payments of proceeds made to third parties overseas, although the transaction is between a domestic buyer and seller, and without apparent legitimate business purpose; (c) PSPM delivered to a third party, who is not the owner or payer of funds, without legitimate business purpose; or (d) Refunds paid to a third party, who is not the owner or payer of funds, without legitimate business purpose. Note: Payments may be in the form of third-party cheques or a third-party credit card. v) Transactions with no apparent business purpose among associates or trading accounts for PSPM and asset-backed tokens traded using bullion, investment or asset-backed token. vi) Large transactions which are cancelled shortly after deposits or full payment are made, resulting in the refunds. For example, the customer may pay for the transaction in cash and request the refund be issued in the form of a cheque. Conversely, the transaction may be made with a credit card and the customer request for the refund to be in cash or other means.	(d) Misclassification of gold purity, weight, origin and value on customs declaration forms. (e) The transaction involves the use of front or shell companies, which have no real operating activity. For example, the entity's ownership structure appears to be doubtful or obscure or the entity refuses to provide additional information when requested. ii) Transactions in which third parties are involved, either as payers or recipients of payment or PSPM, without apparent legitimate purpose. (a) Funds paid to a third party who is not related to the supplier, without legitimate business purpose; or (b) PSPM delivered from a third party who is not related to the supplier, without legitimate business purpose. iii) Transaction involving virtual assets, especially where ownership of the virtual assets cannot be easily traced to the regulated dealer and supplier.

vii)	Overpayment of transactions with a request to refund excess in cash or to a third party.	
viii)	Transactions involving virtual assets, especially where ownership of the virtual assets cannot be easily traced to the customer.	
ix)	Transactions involving the use of stolen or fraudulent payment instruments, for example a payment card that appears stolen or altered or not issued in the customer's name. Some other possible indicators of suspicious online payment 'card-not-present' transactions could include: (a) Same shipping address, but different payment cards: Multiple online orders with mismatched payment card information could signify a criminal attempting to use a series of stolen or fraudulent payment cards while the cards are still active. (b) Same payment account, but different shipping addresses: Some criminals may share stolen payment card information with accomplices, or order PSPM for them and ask for the PSPM to be shipped to various different shipping addresses. (c) Same Internet Protocol address (IP address): Online orders made from the same IP address, especially at or around the same time, but with different payment cards could signify criminals attempting to use fraudulent payment cards. (d) Reattempting with smaller transaction amount: When an online order is flagged as a potential fraud and declined, criminals may attempt to quickly purchase another item that cost less. This may indicate a form of card testing to try identifying the card's limit and available balance of the account.	

Customer Behaviour	**Supplier Behaviour**
i) The customer appears to be structuring amounts to avoid customer identification or reporting threshold. For example, numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial (e.g. below the regulatory threshold for CDD), but the cumulative total of which is substantial. Note: especially if just below S$20,000 cash reporting threshold. ii) The customer makes enquiries about refund policies and requests for large refunds subsequently. iii) The customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes, e.g. the customer presents identification documents with recent issue dates. iv) The customer is unusually concerned with the PSMD's anti-money laundering and countering the financing of terrorism ("AML/CFT") policies. v) The customer fails to provide sufficient explanation and/or documents for the source of funds for his transaction. For example, the customer attempts to use a third-party cheque or credit card in which the source of funds or underlying ownership cannot be easily traced to the customer or is questionable. vi) The customer attempts to maintain a high degree of secrecy with respect to the transaction, for example: (a) To request that normal business records not to be kept; or	i) The supplier is unable to provide information for due diligence and record keeping purposes. ii) The supplier is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes. iii) The supplier's origins of the PSPM appear to be fictitious, doubtful or cannot be explained. For example, the supplier sells a large amount of PSPM that originate or are known to be traded from areas not known for their production i.e. trading centres. iv) The supplier is unusually concerned with the PSMD's AML/CFT policies. v) The supplier attempts to maintain a high degree of secrecy with respect to the transaction, for example – (a) Request that normal business records not to be kept; or (b) Unwillingness to identify beneficial owners or controlling interests, where this would be commercially expected; or (c) Request for payments to be made through money services businesses or other non-bank financial institutions for no apparent legitimate business purposes. (d) Is vague or refuses to provide information on the reason for selling or buying PSPM, or about the origin

(b) The customer is unable or unwilling to provide information for due diligence and record keeping purposes. (c) The customer is unable or unwilling to identify beneficial owners or controlling interest, where this would be commercially expected. (d) The customer is vague or refuses to provide information on the reason for buying or selling PSPM, or about the origin of the items.	of the items.
vii) The customer or the declared owner of the funds is traced to negative news or crime. For example, the person is named in a reliable source (which can include a media or other open sources) that the person is suspected of being involved in illegal activity, or detected when screened against UN Security Council Resolutions (UNSCRs).	vi) (For diamonds only) Rough diamonds are not accompanied by a valid Kimberley Process (KP) certificate. For example: (a) No KP certificate attached to the shipment of rough diamonds; or (b) The KP certificate is or appears to be forged; or (c) The KP certificate has a long validity period.
viii) 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.	vii) The supplier is traced to negative news or crime. For example, the person is named in a reliable source (which can include a media or other open sources) that the person is suspected of being involved in illegal activity, or detected when screened against UN Security Council Resolutions (UNSCRs).
ix) The customer dramatically increases purchases of PSPM for no apparent reason or is willing to sell PSPM at a rate significantly lower than their typical sale value.	viii) The supplier appears to be related to a high-risk country or territory or entity that is associated with risk for money laundering or terrorism activities or a person that has been designated as terrorists.
x) The customer is employed by a PSMD but is dealing in his personal capacity.	ix) The supplier transports the PSPM through a country or territory that is designated as 'high risk for money laundering or terrorism activities' for no apparent economic reason.
xi) The customer uses alternative addresses for delivery such as a General Post Office (GPO), private service provider mailbox or	x) The location to which the PSPM are moved directly to or from storage, is different from the supplier's listed address. xi) The supplier uses alternative addresses such as a General

third parties to receive purchases. xii) The customer appears to be in a hurry to complete the transaction. xiii) The customer purchases PSPM without consideration for the value, size and/or colour of the PSPM or other costs (e.g. the extra expense of rush shipping) in the transaction. xiv) The customer is accompanied by others who appear suspicious (e.g. lurking outside the premise and closely monitoring the customer) and is in doubt when asked for further details. xv) The customer requests to alter the transaction after being asked for identity documents. xvi) The customer makes unnecessary self-disclosure that his funds are clean and not involved in any money-laundering activities. xvii) The customer pays excessively for an item beyond its expected selling price in an auction. xviii) The customer insists on using cash to pay for excessively high value transactions when there was no apparent economic reason.	Post Office (GPO) or private service provider mailbox which appears to be concealing its whereabouts. xii) The supplier appears to be in a hurry to complete transaction or is willing to sell PSPM at a rate significantly lower than their typical sale value. xiii) The supplier does not appear to understand the PSPM industry, or lacks the appropriate equipment or finances to engage in regulated activity in the PSPM industry. xiv) The supplier appears to be uninterested in or uninformed about the structure or transactions of their PSPM business. xv) Other indicators that may warrant closer scrutiny. For example, the supplier offers products such as loose diamonds that retain their wholesale value because they can be easily liquidated. The supplier may insist on offering products through non-face-to-face means (telephone, mail internet). These delivery channels may pose higher risks, as it may make it more difficult to identify the supplier.