

## **Red Flag Indicators for Regulated Dealers**

### **General Comments**

Any person, who in the course of trade, profession, business, or employment, knows or has reasonable grounds to suspect that any property may be connected to a criminal activity, is required to file a Suspicious Transaction Report (“STR”) to the Suspicious Transaction Reporting Office (“STRO”). Failure to file a STR may constitute a criminal offence. The reporting requirement is set out in Section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (also commonly known as CDSA).

Every person in Singapore and every Singapore citizen outside Singapore also have a duty to provide information on property and financial transactions belonging to terrorist and acts of terrorism financing to the Police. This legal obligation is set out in Sections 8 and 10 of the Terrorism (Suppression of Terrorism) Act 2002 (“TSOFA”). Failure to provide information may constitute a criminal offence. The disclosure of terrorism financing information can be made to STRO in a STR.

The list of red flag indicators below is meant to help Precious Stones and Precious Metals Dealers (“PSMDs”) identify some of the circumstances that could be suspicious in nature. They could indicate that property may represent proceeds of money laundering (“ML”) or terrorism financing (“TF”) or proliferation financing (“PF”) or used/intended to be used in connection with ML or TF or PF.

While each individual indicator may not be sufficient by itself to suggest ML or TF or PF, a combination of the indicators may indicate a suspicious transaction. The list is not exhaustive. It may be updated due to changing circumstances and new methods of laundering money or financing terrorism or proliferation financing. Please refer to STRO’s website for the latest list of red flags.

PSMDs should check the plausibility of a customer’s declarations regarding such transactions. PSMDs should not accept every explanation offered by the customer without scrutiny.

There may be reasonable grounds to suspect any customer who is reluctant to provide normal information and documents required routinely by the PSMD before entering into a designated transaction. PSMDs should pay attention to customers who provide minimal, false or misleading information.

### **Red Flag Indicators: Customers**

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.

### **Transaction Patterns**

- i) Transactions that are not consistent with the expected or known profile of the customer:

- (a) Transactions that appear to be beyond the means of the customer based on his/her stated or known occupation or income, experience in the industry or known share capital or period of incorporation; or
  - (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) Unusually large amounts of cash, traveller's cheques, cashier's cheques or precious metals, e.g. gold bars or precious stones, e.g. diamonds, digital payment tokens involved in the transactions.
  - iii) Unusually 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; or
    - (b) Payments received from multiple third parties for the same transaction; or
    - (c) Payments of proceeds made to third parties overseas, although the transaction is between a domestic buyer and seller, and without apparent legitimate business purpose; or
    - (d) PSPM delivered to a third party, who is not the owner or payer of funds, without legitimate business purpose; or
    - (e) 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, a third-party credit card, precious metals, e.g. gold bars or precious stones, e.g. diamonds and digital payment tokens.

- 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.
- 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; or
  - (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; or
  - (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; or
  - (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.
- x) Transactions involving unusual or complex payment arrangements, without apparent legitimate business purpose.
- xi) The transaction involves containers whose numbers have been changed or ships that have been renamed.
- xii) The shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner.
- xiii) The transaction involves the shipment of goods inconsistent with normal geographic trade patterns or consumer patterns (e.g. the country involved would not normally export or import such goods).

### **Customer 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, countering the financing of terrorism and countering proliferation financing ("AML/CFT/CPF") 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
  - (b) The customer is unable or unwilling to provide information for due diligence and record keeping purposes; or
  - (c) The customer is unable or unwilling to identify beneficial owners or controlling interest, where this would be commercially expected; or
  - (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.
- vii) The customer or the declared owner of the funds is traced to adverse 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).
- 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.
- 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.
- x) The customer is employed by a PSMD but is dealing in his personal capacity.
- xi) The customer uses alternative addresses for delivery such as a General Post Office (GPO), private service provider mailbox or 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.
- xix) Customers provided inconsistent information, including in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

## **Red Flag Indicators: Suppliers**

### **Transaction Patterns**

- 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; or
  - (d) Misclassification of gold purity, weight, origin and value on customs declaration forms; or
  - (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) Transactions involving virtual assets, especially where ownership of the virtual assets cannot be easily traced to the regulated dealer and supplier.
- iv) The transaction involves containers whose numbers have been changed or ships that have been renamed.

- v) The shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner.
- vi) The transaction involves the shipment of goods inconsistent with normal geographic trade patterns or consumer patterns (e.g. the country involved would not normally export or import such goods).

### **Supplier Behaviour**

- 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/CPF 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; or
  - (d) Is vague or refuses to provide information on the reason for selling or buying PSPM, or about the origin of the items.
- 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.
- vii) The supplier is traced to adverse 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 UNSCRs.

- 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.
- 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.
- 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 as a GPO, 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.
- xiv) 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.
- xv) Suppliers provided inconsistent information, including in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

## Red Flag Indicators: Proliferation Financing<sup>1</sup>

The following are some of the red flag indicators that could alert PSMDs to customers and transactions that are possibly associated with PF-related activities:

- i) The customer is vague and resistant to providing additional information when asked.
- ii) The customer's activity does not match its business profile or the end-user information does not match the end-user's business profile.
- iii) The transaction involves designated individuals or entities.
- iv) The transaction involves higher risk countries or jurisdictions, or involves other entities with known deficiencies in AML, CFT or CPF controls, or involves possible shell companies.
- v) The transaction involves containers whose numbers have been changed or ships that have been renamed.
- vi) The shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner.
- vii) The transaction involves the shipment of goods inconsistent with normal geographic trade patterns or consumer patterns (e.g. the country involved would not normally export or import such goods).
- viii) There are inconsistencies in the information provided, including in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

The FATF has also provided guidance on measures to combat PF and PSMDs may wish to refer to the [FATF website](#) for additional information.

---

<sup>1</sup> Red flag indicators compiled from MAS's Guidelines to MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism, and Sound Practices to Counter Proliferation Financing.



## Red Flag Indicators: Misuse of Shell and Front Companies<sup>2</sup>

Shell companies are companies (also known as “Legal Persons”) with no operations, assets or business activities. Although all companies start as shell companies, many become fully operational and carry out legitimate business activities. Others may remain as shell companies serving legitimate purposes such as transaction vehicles for corporate mergers or to protect names from being used by others. Generally, a company used for illegitimate or illicit purposes may become more apparent only after its incorporation.

Not all companies that are being misused for money laundering are shell companies. Front companies with a portfolio of businesses, comprising a mix of legitimate and illicit activities, are often used. This makes it challenging to identify the true nature of companies.

When carrying out transactions with Legal Persons, PSMDs should watch out for the following signs of illicit activities.

### **Pass-Through Transactions**

Pass-through transactions create additional layers in attempts to mask the proceeds from illicit activities. Transactions that pass through Legal Persons with no real economic purpose or plausible explanations are risk indicators that the Legal Person may be misused for money laundering.

### **Round-Tripping Activities**

Round-tripping activities are a series of transactions where original funds are passed through entities but eventually returned to original entity, with the pass-through activity serving no apparent economic purpose. The objective is to create the impression that money is derived from legitimate commercial activities.

### **Hidden Relationships**

Relationships between Legal Persons may be hidden using nominee shareholders/directors with complex structures involving listed companies. Such relationships are usually not apparent and PSMDs should be alert to the need for such overly complex relationships or the mixed use of personal and corporate funds in the purchase of PS/PM/PP.

### **Use of Similar Name Entities**

Front companies may be set up, without significant assets or business activity, using similar names to establish entities. The purpose is to give an impression of legitimacy through association, and fake documents may be produced to allow transfer of funds through these front companies.

---

<sup>2</sup> Red flag indicators compiled from MAS’s Risk of Misuse of Legal Persons and ABS’s Legal Persons – Misuse Typology and Best Practices.

### Red Flag Indicators: GST Missing Trader Fraud (“MTF”) Involving Precious Metals<sup>3</sup>

IRAS has observed MTF arrangements involving Investment Precious Metals (“IPM”) gold bars that are exempted from GST. Syndicates will transform the IPM gold bar into scrap gold by melting, cutting or defacing them for onward sale to businesses down the supply chain. A supplier fails to account for or pay the GST charged on his sales (this supplier is referred to as the “**Missing Trader**”), while businesses along the supply chain continue to claim credit of input tax or refund of GST on their purchases. A list of non-exhaustive warning signs and the due diligence checks are provided below.

Warning Signs	Due diligence checks
<ul style="list-style-type: none"> <li>• <b>High-value deals offered by newly established supplier</b>, with minimal experience in the industry.</li> <li>• <b>Very quick turnaround of high-volume transactions</b>, making the business appear unrealistically lucrative.</li> <li>• <b>Back-to-back purchase to sale arrangement</b> with a fixed gold price between the supplier and customers, making the business practically risk free with little or no exposure to price volatility.</li> <li>• <b>Out of the norm credit terms.</b> For example, supplier delivers the gold to you first, and only requires you to make payment after you receive the payment from the customer.</li> <li>• <b>Too good to be true deals recommended by unfamiliar introducer.</b></li> <li>• <b>Scrap gold bars in condition or volume that is not ordinarily traded in the market.</b> For example, buying or selling cut or defaced IPM gold bars or cast scrap gold bars in large quantity.</li> <li>• <b>Supplier/ introducer is evasive</b> when being asked about the source of its gold supply.</li> <li>• <b>Material changes in the transactions with existing suppliers or customers.</b> For example, significant increase in transaction volume or</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Are your immediate supplier and customer legitimate?</b> Obtain business incorporation details, perform credit checks, request for trade references and verify whether they are credible, and visit their business premises.</li> <li>• <b>Is the business arrangement valid?</b> Understand whether there are valid business reasons for IPM gold bars to be defaced or cut and sold as scrap gold bars, whether there are reasonable explanations for the high volume and/or low price of the scrap gold bars relative to the market price and demand, whether the absence of price volatility risk is in line with commercial practice, and whether there is any value for you to be part of the back-to-back purchase to sales arrangement when the customer could have purchased the goods directly from the supplier.</li> <li>• <b>Is the payment arrangement highly favourable?</b> Is there commercial justification for the payment to be made to the supplier only after payment is received from the customer.</li> <li>• <b>Are the scrap gold bars authentic?</b> Question the source of the scrap gold bars and whether there is a reasonable explanation for them to be defaced IPM gold bars.</li> <li>• <b>Is the introducer legitimate and credible?</b> Obtain more information on the introducer. For example, his/her experience in the trade, and the reason</li> </ul>

<sup>3</sup> Red flag indicators compiled from IRAS’s Beware of GST Missing Trader Fraud Involving Precious Metals.

Warning Signs	Due diligence checks
<p>transaction value, or changes in the nature of goods trade.</p> <p>Note: The above risk indicators and due diligence checks are not exhaustive.</p>	<p>for him/her to offer you the deals instead of carrying out the deals himself/herself.</p> <ul style="list-style-type: none"> <li>• <b>Is there a valid reason for material changes in the transactions?</b> Be alert to unusual changes when transacting with existing suppliers and customers. For example, question whether there is any reasonable explanation for the significant increase in the transaction volume and value.</li> </ul>