

We Make Trade Easy, Fair & Secure Circular No: 15/2014

08 Dec 2014

To Traders and Declaring Agents

Dear Sir/Madam

ADVISORY: COMBATING MONEY LAUNDERING AND TERRORISM FINANCING

This advisory serves to remind you on the existing reporting obligations under Singapore's laws and the importance of adopting internal controls and procedures as preventive measures against money laundering (ML) and terrorism financing (TF). A description of ML and TF is at **Annex A**.

Reporting Obligations under Existing Laws

Legal Obligation to File Suspicious Transaction Reports or Police Report

- 2. Under Singapore's laws, all persons are subject to the following reporting obligations relating to anti-money laundering and counter terrorism financing. Any persons, including traders and declaring agents, who contravene the relevant provisions shall be guilty of an offence. The principal laws are as follows:
 - a) Section 39 of the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA): All persons are required to lodge a Suspicious Transaction Report if they know or have reason to suspect in the course of his business or employment that any transaction or the related property is connected to drug dealing or criminal conduct.
 - b) Section 8 and Section 10 of the Terrorism (Suppression of Financing) Act (TSOFA): All persons are required to make a police report if they have information or possess any property pertaining to terrorism financing or terrorist activities.
- 3. Traders and declaring agents are thus required to file a Suspicious Transaction Report or police report in line with the above-mentioned reporting obligations under the existing laws in Singapore, to combat ML and TF.



How to submit Suspicious Transaction Reports

- 4. A list of examples of common indicators of suspicious transactions is provided at **Annex B**. This list of examples is not exhaustive and is meant to guide traders and declaring agents to assess the money laundering or terrorism financing risk of both existing and prospective clients.
- 5. Traders and declaring agents are to submit your Suspicious Transaction Report to the Suspicious Transaction Reporting Office (STRO) of the Commercial Affairs Department. You can lodge a Suspicious Transaction Report in writing (addressed to Head, Suspicious Transaction Reporting Office) or via email to STRO@spf.gov.sg. More details on how to lodge a Suspicious Transaction Report are available on CAD's website through the following link: http://www.cad.gov.sg/reporting/lodging-a-suspicious-transaction-report.

<u>Tipping Off Another Person</u>

6. It is an offence under Section 48 of the CDSA or Section 10B of the TSOFA for any persons, including traders and declaring agents, to tip off another person that a Suspicious Transaction Report or police report has been made or provide any other information to another person that will prejudice investigation or proposed investigation. The penalty for tipping off is imprisonment for a term up to 3 years and/or a court fine up to \$30,000.

<u>Legal Obligation for Record Keeping and Retention of Documents</u>

7. Under Section 90 of the Customs Act and Section 46 of the Goods and Services Tax Act, traders and declaring agents are required to keep documents and records relating to the purchase, importation, sale or exportation of your goods for not less than 5 years.

Internal Controls and Procedures as Preventive Measures

- 8. Traders and declaring agents should adopt robust internal procedures to ensure that your businesses are not being used as a conduit for money laundering and terrorism financing. Some such suggested preventive measures that you may wish to consider are as follows:
 - a) Know Your Customer checks: Under the relevant provisions of the TSOFA, all persons in Singapore, including traders and declaring agents, are prohibited from dealing with terrorists or terrorist-related entities and other entities designated by the United Nations Security Council (UNSC) 1. Hence, it is important for traders and declaring agents to screen both

http://www.un.org/sc/committees/1718/





Page 2 of 9

¹ Examples of publicly available lists which companies can use for customer screening to identify designated entities are:

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

http://www.un.org/sc/committees/1988/pdf/1988List.pdf

http://www.un.org/sc/committees/1737/

- existing and prospective customers against customer screening databases and publicly available lists of individuals and entities known or suspected to be related to a terrorist or a terrorist organisation and its financing.
- b) <u>Carry out on-going due diligence</u>: It is also important for traders and declaring agents to monitor, on an on-going basis, your business relations with clients. Such monitoring, depending on the risk profiles of customers, may involve:
 - Scrutinising transactions undertaken in the course of the business relationship to ensure that the transactions are consistent with the knowledge of the client, its business and risk profile and where appropriate, the source of funds;
 - ii. Paying special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose;
 - iii. Ensuring customer information is kept up to date and relevant particularly for higher risk categories of clients and transactions; and
 - iv. To the extent possible, inquiring into the background and purpose of the transactions and documenting findings with a view to making this information available to the relevant authorities should the need arise.

For further information on Anti-Money Laundering and Counter-Terrorism Financing

- 9. Traders and declaring agents may wish to take appropriate steps to ensure that your staff are regularly and adequately trained on:
 - Anti-money laundering and counter-terrorism financing laws and regulations, in particular, customer due diligence measures, and detecting and reporting of suspicious transactions;
 - b) Prevailing techniques, methods and trends in ML and TF; and
 - c) Internal policies, procedures and controls on anti-money laundering or counter-terrorism financing, and the roles and responsibilities of traders and declaring agents in combating ML and TF.
- 10. More information about anti-money laundering and counter-terrorism financing can be obtained from:
 - a) CAD's AML/CFT webpage at http://www.cad.gov.sg/aml-cft;
 - b) CAD's Anti-Money Laundering and Counter-Terrorism Financing Handbook at http://www.cad.gov.sg/publications/cad-anti-money;



c) CAD's website's 'Frequently Asked Questions' relating to the reporting and detection of Suspicious Transaction Report through the following link: http://www.cad.gov.sg/faqs/reporting/lodging-reports.

For further clarification on Suspicious Transaction Reporting Obligation

11. For further enquiries or clarifications on the Suspicious Transaction Reporting regime, please email to the STRO at STRO@spf.gov.sg.

Yours faithfully

Doreen Tan Assistant Director-General (Policy & Planning) for Director-General of Customs Singapore Customs

This circular is prepared with inputs from the Commercial Affairs Department.

(This is a computer-generated circular. No signature is required.)

We hope that this circular has been written in a way that is clear to you. If not, please let us have suggestions on how to improve this circular at customs_feedback@customs.gov.sg.



Annex A: Description of Money Laundering and Terrorism Financing

Description of Money Laundering

Money laundering can be defined as the process whereby criminals introduce the proceeds of their criminal activities into the world's financial system in an attempt to disguise the true origin of the funds. These funds may be proceeds from drug dealing or other serious crimes. The laundering of tainted funds in this manner allows criminals to use their "dirty money" without fear of detection or prosecution. They can also use these proceeds to fund further crime.

- 2. Generally, an act of money laundering involves three stages:
 - i. Placement: The placement stage of money laundering takes place when there is physical disposal of the benefits (such as cash proceeds) derived from illegal activities of drug dealing or criminal conduct. Here, the money launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited direct into a bank account, or by purchasing a series of monetary instruments (cheques, money orders etc.) that are then collected and deposited into the accounts at another location.
 - ii. Layering: After the funds have entered the financial system, the layering stage takes place. Layering refers to separating illicit proceeds from their source by creating layers of financial transactions designed to disguise the source of money and subvert the audit trail. The funds might be channelled through the purchase and sale of investment instruments/properties, or the money launderer might simply wire the funds through a series of bank accounts across the globe. In some instances, the money launderer might disguise the transfers as payments for goods and services/properties, giving them a legitimate appearance.
 - iii. Integration: Integration is the provision of apparent legitimacy to benefits of drug dealing or criminal conduct. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. The money launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

Description of Terrorism Financing

3. Terrorists require funds to carry out acts of terrorism and terrorism financing provides the funds needed. Sources of terrorism financing may be legitimate or illegitimate. It may be derived from criminal activities such as kidnapping, extortion, fraud or drug dealing. It may also be derived from legitimate income such as



membership dues, sales of publications, donations from persons or entities sympathetic to their cause and sometimes income from legitimate business operations belonging to terrorist organisations.

4. Terrorism financing involves amounts that are not always large and the associated transactions may not necessarily be complex given that some sources of terrorist funds may be legitimate. However, the methods used by terrorist organisations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organisations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organisation would have similar concerns to a typical criminal organisation in laundering the funds. Where the funds are derived from legitimate sources, the terrorist organisations would usually still need to employ the same money laundering techniques to obscure or disguise the links between the organisation and the funds.

Annex B: List of Examples of Common Indicators of Suspicious Transactions

This list of indicators is meant to assist traders and declaring agents to assess the money laundering or terrorism financing risk of both existing and prospective clients. It is not an exhaustive list and the existence of any indicator(s) does not imply that the trade transaction is necessarily linked to such money laundering or terrorism financing activities. If a trader or declaring agent, in the course of business, has reasonable grounds to suspect that any property is linked to criminal conduct, he is required to disclose his suspicion to the Suspicious Transaction Reporting Office (STRO).

Adverse News Relating to ML/TF and Crime

- Client is traced to negative news or crime e.g. he is named in a news report on a crime committed, or detected when screened against UN Security Council Resolutions (UNSCRs).
- Stakeholders²/counterparties of stakeholders found to be linked to known terrorist organisations/money laundering/other offences.

Client Behaviour - Natural Persons (Individuals) and/or Legal Persons (e.g. Companies, Businesses, Trusts, Foundations, Societies and Cooperatives)

- Client appears hesitant or declines to put his name on any document that would connect him with the property/goods.
- Client attempts to hide the identity of the ultimate beneficial owner³ or requests that the transaction be structured to hide the identity of the true client.
- Client provides an address that is unknown, believed to be false, or simply a correspondence address.
- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client queries about the anti-money laundering or counter-terrorism financing reporting requirements.
- Buyer is a shell company⁴ and representatives of the company refuse to disclose the identity of the true owners.

³ Beneficial owner refers to the natural person(s) who ultimately owns or controls (this means situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control) 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.



Page 7 of 9

² Examples of stakeholders include the originator/beneficiaries of the goods imported in/exported out of Singapore, employees, management staff, suppliers, and tenants.

- Client is a recently created legal entity and the amount of the transaction is large compared to their assets.
- Client gave false/misleading explanation for Customer Due Diligence (CDD) purposes.
- Client cannot be contacted for CDD purposes.
- Client is suspected of committing an offence.
- Clients unwilling/unable to provide information for CDD purposes.
- Clients used forged/fraudulent/false identity documents for CDD purposes.

High Risk Transaction Patterns

- Anomalies in payments/transactions that do not correspond with business objectives.
- Nature of bank account transactions does not commensurate with business operations.
- Client pays substantial down payment in cash and the balance is financed by an unusual source or offshore bank.
- Client pays rent or the amount of a lease in advance using a large amount of cash.
- Transaction uses unusual or unnecessarily complex legal structures without any economic logic.
- Details provided by client for the commodity in the bill of lading, invoice and actual shipment of goods have significant discrepancies.
- Client has transactions with entities featured in adverse news/sanction lists.
- Identity of source of funds for client's transactions cannot be immediately known.
- Unable to determine relationship between parties of transaction for CDD purposes.
- Size and type of shipment is inconsistent with the client's and their counterparties' regular business activities.

⁴ Shell companies are companies, registered in Singapore or elsewhere with no legitimate business activities and low paid up capital.





 Client has transactions involving Politically Exposed Persons (PEP) or Associate of PEPs⁵.

Unusual Business Activities/Behaviour

- Lack of business/operational activities.
- Companies registered in Singapore with no apparent business and low paid up capital.
- Goods transferred to beneficiaries with vague/non-specific names.
- Recently established businesses with few or no employees.
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason.
- Circuitous route of shipment and/or circuitous route of financial transaction.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns.

Page 9 of 9



⁵ Politically Exposed Persons (PEPs)

[&]quot;Politically exposed person" means a domestic politically exposed person, foreign politically exposed person or international organisation politically exposed person.

[&]quot;Domestic politically exposed person" means a natural person who is or has been entrusted domestically with prominent public functions.

[&]quot;Foreign politically exposed person" means a natural person who is or has been entrusted with prominent public functions by a foreign country.

[&]quot;International organisation politically exposed person" means a natural person who is or has been entrusted with prominent public function by an international organisation.

[&]quot;International organisation" means an entity established by formal political agreements between member countries that have the status of international treaties, whose existence is recognised by law in member countries and who is not treated as a resident institutional unit of the country in which it is located.

[&]quot;Prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil or public servants, senior judicial or military officials, senior executives of state owned corporations, senior political party officials, members of the legislature and senior management of international organisations.