QUICK GUIDE

Suruhanjaya Sekuriti
Securities Commission
Malaysia

IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS RELATING TO PROLIFERATION FINANCING FOR REPORTING INSTITUTIONS IN THE CAPITAL MARKET

[First Issued: 29 October 2019]
[Revised: 3 September 2024]

1. What is proliferation financing (PF)?

In essence, PF is an act of providing funds or financial services which are used to develop nuclear, chemical or biological weapons and any related materials to weapons of mass destruction (WMD).

2. What is targeted financial sanctions (TFS)?

Asset freezing, blocking and rejection of transactions and persons to prevent, suppress, and disrupt the proliferation of WMD and its financing in line with sanctions imposed by the United Nations Security Council (UNSC) through its resolutions (UNSCR).

3. What are the relevant UNSCRs for TFS-PF?

Democratic People's Republic of Korea / North Korea (DPRK) – Resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016) and 1718 (2024) and their successors.

4. What are the main legislations in Malaysia for TFS-PF?

- The Strategic Trade Act 2010
- The Strategic Trade (UNSCR) Regulations 2010
- The Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010
- The Strategic Trade Controller Directive Amendment 2024 (Link: TARGETED FINANCIAL SANCTIONS RELATING TO PROLIFERATION FINANCING (TFS-PF) (miti.gov.my))

5. What is PF Risk?

- PF risk is limited to potential breach, non-implementation or evasion of the TFS-PF under Part VIII of the SC's *Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Reporting Institutions in the Capital Market* which was revised on 13 June 2024 (AML Guidelines).

6. How do intermediaries identify, assess and understand PF risks via institutional PF risk assessment?

- Intermediaries must take appropriate steps to identify, assess and understand PF risks in relation to the following:
  - customers
  - countries or geographical areas
  - products, services, transactions or delivery channels
  - other relevant risk factors where the extent of the assessment shall be appropriate to the nature, size and complexity of its business.
- In conducting risk assessment, an intermediary need not necessarily establish a standalone or new PF risk framework/methodology but may consider if its existing money laundering or terrorism financing risk assessment framework/methodology are applicable and adequate towards its assessment of PF risks.

7. What are the main obligations that intermediaries must comply with under the SC's AML Guidelines?

A. To maintain sanctions list

- Keep itself updated of various UNSCR and the list of designated persons on TFS-PF.
- Maintain updated and current database of name and particulars of the designated persons.

Guidance

- **Designated persons**: persons subject to measures imposed by UNSC.
- The list of designated persons on TFS-PF is specified in the UN Consolidated List and it is applied automatically via reference to the updated list in the UN website.
- Refer to the link for updated UN Consolidated List: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

- Reporting institutions may consider subscribing to electronic subscription service to maintain the updated UNSCR.

B. To conduct screening on customers

- Conduct screening on existing, new and potential customers to check for any positive name matched with any designated person.
- Screen its entire customer database **without delay** when new names are listed on a UNSCR.
- Screening also includes funds derived from property owned or controlled by designated person or its related party.
- When there is a name match, reasonable measures must be taken to verify and confirm the identity of the customer against the designated person.

Guidance

- **Without delay**: a matter of hours of a designation by UNSC.
- Intermediaries are advised to search, examine and analyse past financial activities of designated person or related party.
- Always be wary of the possible use of false identities, dua nationalities, multiple names and identities.
- Intermediaries are encouraged to conduct PF risk assessment.

C. To freeze, block and reject

- Existing customers – once the identity is matched with the designated person, intermediary must freeze funds, properties or accounts.
- Potential or new customer – once the identity is matched with the designated person, intermediary must reject the customer if the transaction has not commenced.
- Where **"false positive"** scenario exists, the affected person may make an application to the Strategic Trade Controller to unfreeze such assets.
- The freezing shall remain in effect until the person is delisted or it is confirmed that it is a "false positive".

Guidance on "False Positives"

- **"False positive"**: where a customer's name is similar to the name of a designated person, but he is not the designated person.
- Intermediaries may forward queries to SC to determine whether the customer is a designated person.
- Such query must include additional info, copies of ID and relevant analysis.
- Intermediaries should advice affected customer to contact Strategic Trade Controller to verify the false positive match.

Guidance on the Freezing of Funds

- If assets jointly owned by designated person cannot be segregated, entire asset should be subject to freezing.
- Frozen assets can continue to receive dividends, interest etc, but such benefit must remain frozen.
- No outgoing payment should be made from the frozen funds without prior authorisation of Strategic Trade Controller.

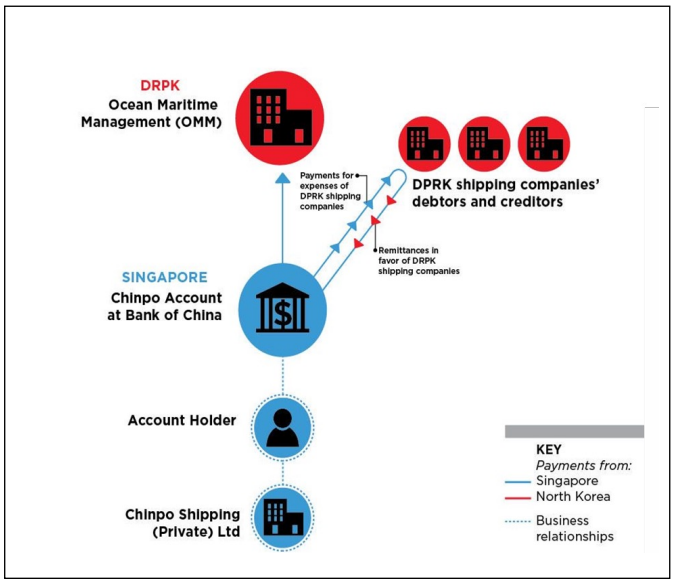
D. To report to authorities

- Reporting to SC: Intermediaries must immediately report on any freezing, blocking or rejection actions taken.
- Reporting to Financial Intelligence and Enforcement Department (FIED) of Bank Negara Malaysia (BNM): Intermediaries must submit Suspicious Transaction Report (STR) in the following circumstances:
  - Positive name matches arising from on-going screening of customer database.
  - When there is an attempted transaction by any of the designated person or its related party.
- Intermediaries who have reported name matches and has control of frozen assets must report to SC on any **change to the frozen assets** by 31 January in the next calendar year.

Guidance

- Change to frozen assets includes interest payment or dividends pay outs.

8. Example of a Proliferation Financing Case: DPRK Entity using a company outside DPRK as a payment agent



- In June 2014, Chinpo Shipping Co (Pte) Ltd (Chinpo) was charged in Singapore for transferring money to facilitate shipment of items that could reasonably have been used to contribute to the nuclear related programmes or activities of DPRK (PF related charge).
- In June 2013, a ship "MV Chong Chon Gang" was stopped in the Panama Canal on its way from Cuba to DPRK. The ship was managed by a DPRK shipping company, Ocean Maritime Management (OMM).
- The Panaman authorities found 25 containers of military equipment including MiG-21 fighter jets and surface to air-missile systems concealed beneath over 10,500mt of sugar in the ship.
- Investigations revealed that Chinpo paid US$72,016.76 to a Panama Canal shipping agent through Chinpo's Bank of China account for the ship's passage through the Panama Canal, on behalf of OMM.

Other investigation findings

- Chinpo's director, Tan Cheng Hoe (Tan) had been providing services related to DPRK maritime trade since the 1980s, and OMM became Chinpo's primary client since 1990s. OMM was later sanctioned by UN for proliferation financing in July 2014.
- Tan allowed his office address to be used as the DPRK Embassy postal address in Singapore.
- Between 2009 and 2013, Chinpo also has made outward remittances on behalf of OMM and other DPRK entities from its Bank of China's account amounting to US$40 million, charging a fee of at least US$50 per transaction in most occasions. For this, Chinpo was charged for carrying out unlicensed remittance business.
- Tan would withhold the name of the DPRK ship in the Bank of China's wire transfer form to avoid suspicion. The court documents also recorded that Bank of China rarely queried remittance made by Chinpo.

Court's decision

- Chinpo was convicted at the court of first instance for the PF related charge and for carrying out unlicensed remittance business. On appeal, the conviction for the PF-related charge was overturned on the basis that it was not reasonable that the cargo of weapons on board of the ship could reasonably be used in DPRK's nuclear programmes.

8.1 Key lessons from the case

Key lessons relevant for intermediaries:

- An intermediary should ensure proper and effective customers due diligence where it would be able to–

  (a) detect customer who may be controlled by a person who may be involved in proliferation of WMD network; and
  (b) recognise/ detect the inconsistencies between the customer's economic profile and the amount of funds in its accounts (e.g. In Chinpo - a small, family-run shipping company vs. the massive circulation of funds in its account).

- Early detection would allow the intermediary to take action to curtail further dealings with the customer.
- Considering the risk associated with a customer (who have dealings with a person who may be involved in proliferation of WMD network) the intermediary may regard it as a high-risk customer and conduct enhanced due diligence (e.g: inquiring more information on purpose of transaction).
- If an intermediary could not mitigate the risks posed by the customer, the intermediary should have considered terminating its business relationship with the customer and filing one or more STRs with relevant authorities.

8.2 Conclusion

- Robust implementation of TFS-PF will prevent, suppress, and disrupt the proliferation of WMD and its financing.
- An intermediary should consider submitting an STR to FIED if it encounters similar circumstances as per the case above. Please refer to Appendix C of the SC's AML Guidelines for more information on how to submit an STR to FIED.
- For examples of situations or transaction indicating PF, please refer to the *FATF Guidance on Counter Proliferation Financing*. Some of the examples from the FATF Guidance are highlighted in item 9 of this Quick Guide.
- Where in doubt, intermediaries should conduct enhanced due diligence measures to verify any suspicion including understanding the nature of relationship and the ownership structure of a customer or any third parties that the customer has any dealing with.

9. Situations indicating possible PF activities

1. Transaction involves person or entity in foreign country of proliferation concern.
2. Transaction involves person or entity in foreign country of diversion concern.
3. The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
4. Customer activity does not match business profile, or end-user information does not match end-user's business profile.
5. A freight forwarding firm is listed as the product's final destination.
6. Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
7. Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
8. Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).
9. Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
10. Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
11. Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
12. Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
13. Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
14. Transaction involves financial institutions with known deficiencies in anti-money laundering / countering terrorism financing (AML/CFT) controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
15. Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
16. Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
17. Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
18. Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
19. New customer requests letter of credit transaction awaiting approval of new account.
20. Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
21. Involvement of items controlled under WMD export control regimes or national control regimes.
22. Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/ or dealing with complex equipment for which he/ she lacks technical background.
23. Use of cash or precious metals (e.g. gold) in transactions for industrial items.
24. Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.

25. Involvement of a customer or counterparty, declared to be a commercial business, whose transactions suggest they are acting as a money remittance business.
26. Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.
27. Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
28. Involvement of a university in a country of proliferation concern.
29. Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
30. Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.
31. Use of personal account to purchase industrial items.

FATF Guidance On Counter Proliferation Financing is available at
http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf